FESTSKRIFT

UDGIVET AF

KJØBENHAVNS UNIVERSITET

I ANLEDNING AF

UNIVERSITETETS AARSFEST

NOVEMBER 1907

JULIUS PETERSEN:

OM DE KVADRATISKE RESTERS SUM OG FORDELING FOR PRIMTAL AF FORMEN 4n + 3

KJØBENHAVN
TRYKT I UNIVERSITETSBOGTRYKKERIET (J. H. SCHULTZ)
1907

FESTSKRIFT

UDGIVET AF

KJØBENHAVNS UNIVERSITET

I ANLEDNING AF

UNIVERSITETETS AARSFEST

NOVEMBER 1907

JULIUS PETERSEN:

OM DE KVADRATISKE RESTERS SUM OG FORDELING FOR PRIMTAL AF FORMEN 4n + 3

KJØBENHAVN
TRYKT I UNIVERSITETSBOGTRYKKERIET (J. H. SCHULTZ)
1907

OM DE
KVADRATISKE RESTERS SUM OG FORDELING

FOR

PRIMTAL AF FORMEN $4n+3$

AF

JULIUS PETERSEN

KJØBENHAVN
TRYKT I UNIVERSITETSBOGTRYKKERIET (J. H. SCHULTZ)
1907

QA242
P48
Mathematics

FØRSTE KAPITEL.

INDLEDNING.

1. For at gøre de følgende Undersøgelser af forskellige Forhold ved de kvadratiske Rester mere overskuelige og sammenhængende, vil jeg først aftrykke et Par af mine tidligere herhen hørende Afhandlinger, nemlig et Bevis for den udvidede Reciprocitetssætning (Tidsskrift for Matematik 1879) og Undersøgelse af Divisorerne i visse kvadratiske Former (Tidsskr. f. M. 1871).

Ved en kvadratisk Rest for Primtallet p forstaa vi et Tal, som vi kunne tænke os mindre end p, og som for Mod. p er kongruent med et Kvadrattal. Opløfte vi alle Tallene, mindre end p, til 2. Potens, og tage vi for hvert af Kvadraterne den mindste positive Rest, faa vi $p-1$ Tal, der ere kvadratiske Rester for p, men, da α^2 og $(p-\alpha)^2$ ere kongruente, blive kun $^1/_2(p-1)$ af Tallene forskellige; de andre $^1/_2(p-1)$ Tal kaldes Ikkerester; ved Bogstaverne $R.$ og $I.$ (r og i) betegne vi henholdsvis Rester og Ikkerester.

Er $a \equiv \alpha^2$ (mod. p), bliver

$$a^{\frac{p-1}{2}} \equiv \alpha^{p-1} \equiv 1 \qquad (1)$$

ifølge *Fermats* Sætning. For Ikkeresterne b maa man derfor have $b^{\frac{p-1}{2}} \equiv -1$, og vi have derved et Middel til at undersøge, om et givet Tal er $R.$ eller $I.$ Denne Prøve er imidlertid praktisk talt uigennemførlig, saa snart p er et nogenlunde stort Tal. En betydelig Lettelse opnaaedes ved *Legendres* Reciprocitetssætning, der fører til en Algoritme, ved hvilken

Apr. 1, 1932
32715-6

man stadig reducerer Opgaven til den samme Opgave for lavere Tal. Legendre gav intet Bevis for sin Sætning, men *Gauss* gav senere seks saadanne, grundede paa meget forskellige Principer. Metoden naaede imidlertid først sin fulde Betydning ved en Udvidelse af *Jacobi*. Det Bevis, vi her skulle give, slutter sig nærmest til Gauss's tredje Bevis, hvad det har fælles med nogle andre, senere fremkomne, Beviser, men medens disse kun bevise Sætningen i dens oprindelige Form, gælder Forfatterens for Sætningen i dens største Almindelighed. At Opgaven her er formuleret paa en anden Maade end hos Jacobi, vil vise sig som en Lettelse. Efter disse almindelige Bemærkninger gaa vi over til Beviset for

I. DEN UDVIDEDE RECIPROCITETSSÆTNING.

2. Lad a og b være to hvilke som helst indbyrdes primiske Tal, b ulige, Tallene

$$a, 3a, 5a \ldots . (b-2)a$$

divideres med b saaledes, at man faar lutter ulige Rester, beliggende mellem $-b$ og $+b$; dette kan man altid opnaa ved at tage Kvotienterne lige eller ulige, eftersom a er ulige eller lige, og forøvrigt af en passende Størrelse. Resterne maa alle være numerisk forskellige, thi hvis to af dem vare numerisk lige store, maatte b gaa op i Summen eller Differensen af to af de ulige Tal, med hvilke a er multipliceret; dette er imidlertid umuligt, da baade Differensen og Summen ere lige Tal, mindre end $2b$. Resterne maa derfor netop være de ulige Tal, med hvilke vi have multipliceret a, kun at nogle af dem ere negative. Ved Tegnene

$$\left(\frac{a}{b}\right) = +1 \text{ og } \left(\frac{a}{b}\right) = -1, \tag{2}$$

ville vi nu betegne henholdsvis, at de negative Rester forekomme i lige eller ulige Antal.

At de Tegn, jeg her benytter, ere de samme som de Legendreske Symboler, kan ikke foraarsage Misforstaaelser, thi de stemme overens i de Tilfælde, hvor Legendres Tegn overhovedet

have Betydning, nemlig, naar b er et Primtal; man faar nemlig i dette Tilfælde ved Multiplikation

$$1 . 3 . 5 \ldots (b-2)\, a^{\frac{b-1}{2}} \equiv \pm 1 . 3 . 5 \ldots (b-2) \pmod{b},$$

eller

$$1 . 3 . 5 \ldots (b-2)\,(a^{\frac{b-1}{2}} \mp 1) \equiv 0 \pmod{b},$$

der viser, at, naar b er et Primtal, maa det gaa op i

$$a^{\frac{b-1}{2}} \pm 1,$$

eller, at, naar b er et Primtal, de to Betegnelser henholdsvis svare til, at a er *R.* eller *I.* ligesom hos *Legendre*; er b ikke noget Primtal, faar Symbolerne ikke noget med *R.* eller *I.* at gøre, men angive kun, at Antallet af negative Rester ved Divisjonerne er henholdsvis lige eller ulige, og her have vi den fra Jacobi forskellige Formulering af Opgaven, som vi ovenfor omtalte. For a kan man naturligvis sætte ethvert med a for Mod. b kongruent Tal.

Vi sætte nu $a = a_1 a_2$ og behandle a_1 som før a; vi faa derved

$$1 . 3 . 5 \ldots (b-2)\, a_1^{\frac{b-1}{2}} \equiv \left(\frac{a_1}{b}\right) 1 . 3 . 5 \ldots (b-2) \pmod{b}$$

eller, hvis Ligningerne, før de multipliceres med hinanden, alle først multipliceres med a_2,

$$1 . 3 . 5 \ldots (b-2)\, a^{\frac{b-1}{2}} \equiv \left(\frac{a_1}{b}\right) . 1 . 3 . 5 \ldots (b-2)\, a_2^{\frac{b-1}{2}},$$

hvoraf

$$\left(\frac{a}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right). \tag{3}$$

3. Før vi gaa videre, ville vi betragte et Par specielle Tilfælde:

Af Ligningen

$$\left(\frac{k^2}{b}\right) = \left(\frac{k}{b}\right)\left(\frac{k}{b}\right)$$

se vi, at vi af Tallet i Tælleren kunne bortdividere et Kvadrat, uden at Symbolets Værdi forandrer Fortegn.

have Betydning, nemlig, naar b er et Primtal; man faar nemlig i dette Tilfælde ved Multiplikation

$$1 . 3 . 5 \ldots (b-2)\, a^{\frac{b-1}{2}} \equiv \pm 1 . 3 . 5 \ldots (b-2) \pmod{b},$$

eller

$$1 . 3 . 5 \ldots (b-2)\, (a^{\frac{b-1}{2}} \mp 1) \equiv 0 \pmod{b},$$

der viser, at, naar b er et Primtal, maa det gaa op i

$$a^{\frac{b-1}{2}} \pm 1,$$

eller, at, naar b er et Primtal, de to Betegnelser henholdsvis svare til, at a er *R.* eller *I.* ligesom hos *Legendre*; er b ikke noget Primtal, faar Symbolerne ikke noget med *R.* eller *I.* at gøre, men angive kun, at Antallet af negative Rester ved Divisjonerne er henholdsvis lige eller ulige, og her have vi den fra Jacobi forskellige Formulering af Opgaven, som vi ovenfor omtalte. For a kan man naturligvis sætte ethvert med a for Mod. b kongruent Tal.

Vi sætte nu $a = a_1 a_2$ og behandle a_1 som før a; vi faa derved

$$1 . 3 . 5 \ldots (b-2)\, a_1^{\frac{b-1}{2}} \equiv \left(\frac{a_1}{b}\right) 1 . 3 . 5 \ldots (b-2) \pmod{b}$$

eller, hvis Ligningerne, før de multipliceres med hinanden, alle først multipliceres med a_2,

$$1 . 3 . 5 \ldots (b-2)\, a^{\frac{b-1}{2}} \equiv \left(\frac{a_1}{b}\right) . 1 . 3 . 5 \ldots (b-2)\, a_2^{\frac{b-1}{2}},$$

hvoraf

$$\left(\frac{a}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right). \tag{3}$$

3. Før vi gaa videre, ville vi betragte et Par specielle Tilfælde:

Af Ligningen

$$\left(\frac{k^2}{b}\right) = \left(\frac{k}{b}\right)\left(\frac{k}{b}\right)$$

se vi, at vi af Tallet i Tælleren kunne bortdividere et Kvadrat, uden at Symbolets Værdi forandrer Fortegn.

Er $a = -1$, blive alle Resterne negative, og man har saaledes

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}. \tag{4}$$

Er $a = 2$, faa vi Rækken af Tal

$$1 \cdot 2, 3 \cdot 2, 5 \cdot 2, \ldots . (b-2)\,2,$$

der give negative Rester, saa længe Produkterne ere mindre end b. Disses Antal bliver lige, hvis b er af en af Formerne $8n+1$ og $8n+7$, ulige, hvis b er af en af Formerne $8n+3$ og $8n+5$.

Dette udtrykkes ved Ligningen

$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}. \tag{5}$$

4. Vi vende nu tilbage til det almindelige Tilfælde, hvor vi dog kunne forudsætte, at a er ulige, da vi ved (5) kunne bortskaffe Faktoren 2. Endvidere kunne vi forudsætte $a < b$, da vi i modsat Fald for a kunne sætte det med a for Mod. b kongruente Tal, mindre end b. Vi faa da ved Divisjon Ligninger af Formen

$$(2n+1)\,a - 2mb = \nu, \tag{6}$$

hvor $2n+1$ har Værdierne

$$1 \cdot 3 \cdot 5 \ldots (b-2),$$

medens den højeste Værdi for $2m$ er $a-1$. Den samme Værdi af $2m$ kan findes i flere paa hinanden følgende Ligninger, og de tilsvarende Rester danne da en Differensrække med Differensen $2a$. Der maa derfor for enhver Værdi af $2m$ findes netop een Rest, som ligger mellem $-a$ og $+a$.

Ligningerne kunne omskrives til

$$(a-2m)\,b - (b-2n-1)\,a = \nu, \tag{7}$$

hvor $a-2m$ efterhaanden faar Værdierne

$$1, 3, 5, (a-2),$$

og Ligningerne saaledes netop ere de Ligninger, der bestemme

$\left(\frac{a}{b}\right)$; vi gaa imidlertid kun ud paa at bestemme Forholdet mellem $\left(\frac{a}{b}\right)$ og $\left(\frac{b}{a}\right)$ og kunne derfor udelade alle Rester r, der benyttes begge Steder, det vil sige de Rester, der ligge mellem $-a$ og $+a$. Da nu Resterne mellem $+a$ og $+b$ ere positive, behøve vi kun at betragte de Rester, der ligge mellem $-b$ og $-a$; eftersom disse Resters Antal er lige eller ulige, ville de to Symboler have samme eller forskelligt Fortegn. Vi skulle altsaa kun betragte de Værdier af m og n, for hvilke

$$-b < (2n+1)a - 2mb < -a,$$

der, naar vi sætte

$$a = b - 2\alpha,\ m = n - k,$$

omskrives til

$$2n+1 < \frac{(k+1)b}{\alpha} < 2n+2.$$

Da den største Værdi af $2n+1$ er $b-2$, medens $b-1$ er den største Værdi af $2n+2$, bliver $\alpha - 1$ den største Værdi af $k+1$, medens k ikke kan være negativ. Vi have saaledes Rækken af Brøker

$$\frac{b}{\alpha}, \frac{2b}{\alpha}, \frac{3b}{\alpha} \ldots \frac{(\alpha-1)b}{\alpha},$$

og enhver af disse bestemmer en negativ Rest mellem $-b$ og $-a$, dersom dens nærmest lavere hele Tal er ulige. Det gælder altsaa om at finde, om det Antal af Brøkerne, der har den angivne Egenskab, er lige eller ulige.

Nu er imidlertid Summen af den første og den sidste, af den næstførste og den næstsidste Brøk og saaledes videre, lig b, som er et ulige Tal, og to saaledes parrede Brøker maa derfor begge have deres nærmest lavere hele Tal lige eller begge ulige, og de kunne derfor ved den søgte Fortegnsbestemmelse begge udelades.

Hvis nu α er ulige, blive paa denne Maade alle Brøkerne parrede og det søgte Antal negative Rester er lige. Dette Tilfælde indtræder, naar af de to ulige Tal a og b det ene er af

Formen $4n+1$, det andet af Formen $4n+3$. Er a lige, beroer Resultatet paa det mellemste, der er $^1/_2 . b$. b og a ere begge af Formen $4n+1$ eller begge af Formen $4n+3$. I det første Tilfælde er det største hele Tal i $^1/_2 b$ lige og bestemmer derfor ingen negativ Rest, medens det bestemmer en saadan i det andet Tilfælde, da det største hele Tal i $^1/_2 b$ er ulige.

Vi have saaledes bevist, at vi have

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$$

i alle Tilfælde, undtagen, naar de ulige Tal a og b begge ere af Formen $4n+3$. Dette kan udtrykkes ved Ligningen

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}. \tag{8}$$

Regningerne blive nu omtrent de samme som ved Bestemmelse af de to Tals største fælles Maal. Saaledes faa vi f. Eks.

$$\left(\frac{365}{1847}\right) = \frac{1847}{365} = \frac{22}{365} = \left(\frac{2}{365}\right)\left(\frac{11}{365}\right) = -\left(\frac{11}{365}\right)$$
$$= -\left(\frac{365}{11}\right) = -\left(\frac{2}{11}\right) = 1,$$

saa at 365 er $R.$ for Primtallet 1847.

II. DE LINEÆRE FORMER AF DE PRIMTAL, FOR HVILKE ET GIVET TAL ER $R.$ GENNEMFØRELSE FOR DE LAVESTE TAL.

5. -1 er $R.$ for $p = 4n+1$, $I.$ for $p = 4n+3$.

Man har nemlig henholdsvis (4)

$$\left(\frac{-1}{4n+1}\right) = (-1)^{2n} = +1 \text{ og } \left(\frac{-1}{4n+3}\right) = (-1)^{2n+1} = -1.$$

For Tallet 2 have vi (5)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

der viser, at 2 er *R.*, naar $p^2 - 1$ er delelig med 16. Tal af Formen $8n - \alpha$, kunne kun være Primtal for $\alpha = 1, 3, 5, 7$. For $\alpha = 1$ og 7 tilfredsstilles Betingelsen;

$$2 \text{ er derfor } R. \text{ for } p = 8n + 1 \text{ og } 8n + 7,$$
$$I. \text{ for } p = 8n + 3 \text{ og } 8n + 5.$$

Skal -2 være *R.*, maa -1 og 2 begge være *R.* eller begge *I.* Altsaa

$$-2 \text{ er } R. \text{ for } p = 8n + 1 \text{ og } 8n + 3,$$
$$I. \text{ for } p = 8n + 5 \text{ og } 8n + 7.$$

For at undersøge Tallet 3, betragte vi Tallene $12n + \alpha$, hvor $\alpha = 1, 5, 7, 11$; vi have

$$\left(\frac{3}{12n+1}\right) = \left(\frac{1}{3}\right) = 1, \left(\frac{3}{12n+5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

$$\left(\frac{3}{12n+7}\right) = -\left(\frac{7}{3}\right) = -1; \left(\frac{3}{12n+11}\right) = -\left(\frac{11}{3}\right) = +1,$$

altsaa

$$3 \text{ er } R. \text{ for } p = 12n + 1 \text{ og } 12n + 11,$$
$$I. \text{ for } p = 12n + 5 \text{ og } 12n + 7,$$

og følgelig

$$-3 \text{ er } R. \text{ for } p = 6n + 1, \; I. \text{ for } p = 6n - 1.$$

For at undersøge 5, betragte vi Tallene $10n + \alpha$; $\alpha = 1$, 3, 7, 9 og faa $\left(\frac{5}{10n+\alpha}\right) = \left(\frac{\alpha}{5}\right)$, der for $\alpha = 1$ og 4 giver $+1$, for $\alpha = 2$ og 3 giver -1; altsaa

$$5 \text{ er } R. \text{ for } p = 10n + 1 \text{ og } 10n + 9,$$
$$I. \text{ for } p = 10n + 3 \text{ og } 10n + 7,$$

og følgelig

$$-5 \text{ er } R. \text{ for } p = 20n + 1, \; 20n + 3, \; 20n + 7, \; 20n + 9,$$
$$I. \text{ for } p = 20n + 11, 13, 17, 19.$$

I Almindelighed faa vi for $p = 4n + 1$, $\alpha = 1, 2, 3 \ldots p - 1$ $\left(\frac{p}{np+\alpha}\right) = \left(\frac{\alpha}{p}\right) = +1$ eller -1, eftersom α er *R.* eller *I.* for p; da imidlertid, eftersom n er lige eller ulige, α maa være

ulige eller lige, sættes bedre $2n$ for n; α er da ulige, men gaar til $2p$; er $p = 4n + 3$, tage vi for det søgte Primtal Formen $4np + \alpha$ for lettere at se, naar Symbolet skal skifte Tegn ved Brøkens Omvending.

6. Vi kunne ad denne Vej udlede Formen af Primfaktorer i Tal af Formen $x^2 + ay^2$, hvor x er primisk med ay. Sætte vi nemlig, idet k er en Primfaktor i Tallet,

$$yz \equiv x \pmod{k},$$

bestemmes derved en Værdi af z, og vi faa

$$x^2 + ay^2 \equiv y^2z^2 + ay^2 = y^2(z^2 + a) \pmod{k},$$

der, da k ikke gaar op i y, viser, at

En Primfaktor, der findes i et Tal $x^2 + ay^2$, hvor x er pr. med ay findes ogsaa i et Tal af Formen $x^2 + a$.

Vi faa saaledes, idet vi stadig forudsætte x pr. med y og med a og undtage Faktoren 2,

Alle Primfaktorer i $x^2 + y^2$ ere af Formen $4n + 1$.

Alle Primfaktorer i $x^2 - 2y^2$ ere af Formerne $8n \pm 1$.

Alle Primfaktorer i $x^2 + 2y^2$ ere af Formerne $8n + 1$ og $8n + 3$.

Alle Primfaktorer i $x^2 - 3y^2$ ere af Formerne $12n \pm 1$.

Alle Primfaktorer i $x^2 + 3y^2$ ere af Formen $6n + 1$.

Alle Primfaktorer i $x^2 - 5y^2$ ere af Formerne $10n \pm 1$

og saaledes videre.

Fermat angav uden Bevis de Tal, for hvilke -1 og ± 2 ere R.*). Bevis søgtes uden Held af *Euler*, men fandtes af *Lagrange*, der ogsaa undersøgte Tallene ± 3, ± 5, ± 7**); hans Fremgangsmaade var meget besværlig.

---

*) Opera Math. Pg. 168.

**) Nouv. Mém. de l'Acad. de Berlin 1775.

Kvadratiske Rester og Ikkerester for de første Primtal:

5 1 2 3 4. **7** 1 2 3 4 5 6. **11** 1 2 3 4 5 6 7 8 9 10. **13** 1 2 3 4 5 6 7 8 9 10 11 12. **17** 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16.

19 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18. **23** 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22.

29 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28.

31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30.

37 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36.

41 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40.

43 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42.

47 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46.

For de følgende Primtal anføres kun Tallene, mindre end $\frac{1}{2}p$:

53 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 . . .

59 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 . . .

61 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30.

67 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33.

71 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35.

79 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39.

83 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41.

89 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44.

97 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48.

7. Tal af Formen $x^2 + cy^2$ have den mærkelige Egenskab, at Produktet af to saadanne (med samme Værdi af c) kan skrives under samme Form; man har nemlig identisk

$$(9) \qquad (a + b\sqrt{-c})(m \mp n\sqrt{-c}) = x + y\sqrt{-c},$$

hvor

$$(10) \qquad x = am \pm cbn;\ y = bm \mp an$$

og ligeledes

$$(11) \qquad (a - b\sqrt{-c})(m \pm n\sqrt{-c}) = x - y\sqrt{-c}.$$

Ved Multiplikation af de to Ligninger faa vi

$$(12) \qquad (a^2 + cb^2)(m^2 + cn^2) = x^2 + cy^2,$$

hvor vi forudsætte, at alle Tallene ere hele. Vi kunne nu bevise følgende Sætning:

Dersom i et Tal $x^2 + cy^2$ en Primfaktor har samme Form, maa den anden Faktor ogsaa have den.

Man faar nemlig af Ligningerne (10),

$$(13) \qquad a = \frac{mx \pm cny}{m^2 + cn^2};\ b = \frac{nx \mp my}{m^2 + cn^2},$$

hvor vi faa de dobbelte Fortegn ved at tage y baade positiv og negativ, medens Fortegnene for a og b, der skulle kvadreres, ere ligegyldige. Nu gaar $m^2 + cn^2$ op i

$$m^2(x^2 + cy^2) - cy^2(m^2 + cn^2) = (mx + cny)(mx - cny)$$

og i

$$n^2(x^2 + cy^2) - y^2(m^2 + cn^2) = (nx + my)(nx - my).$$

Hvis nu $m^2 + cn^2$ er et Primtal, maa det gaa op i en af Faktorerne i hvert af disse Produkter, saa at een Værdi af a og een Værdi af b ere hele Tal, og at disse ere de sammenhørende Værdier følger af Identiteten

$$(mx \pm cny)^2 + c(nx \mp my)^2 = (m^2 + cn^2)(x^2 + cy^2),$$

der viser, at naar Primtallet $m^2 + cn^2$ gaar op i $nx \mp my$, gaar det ogsaa op i $mx \pm cny$.

8. Da der til et Par hele Værdier af x og y saaledes svarer et Par hele Værdier af a og b, maa man ved at benytte (9) eller (10), faa alle Værdier af x og y, naar man har alle Værdier af a og b, altsaa:

Naar man multiplicerer et Primtal $m^2 + cn^2$ med et vilkaarligt Tal $a^2 + cb^2$ ved Anvendelse af (9) eller (10), faar man Produktet skrevet paa alle mulige Maader, naar man har $a^2 + cb^2$ skrevet paa alle Maader.

Heraf følger atter:

Alle Løsninger af $x^2 + cy^2 = p$, hvor p er et Primtal, faas af een Løsning og af alle Løsninger af $x^2 + cy^2 = 1$.

For c positiv har den sidste Ligning kun Løsningen $x = 1$, $y = o$ (idet vi ikke gøre Forskel paa $+1$ og -1, der give samme Værdi for x^2), altsaa:

Et Primtal kan kun paa een Maade skrives paa Formen $x^2 + cy^2$, naar c er positiv.

Dette forudsætter naturligvis, at $-c$ er kvadratisk Rest for p; i modsat Fald har Ligningen ingen Løsninger. Er c positiv, faar saaledes Ligningen

$$x^2 + cy^2 = A \tag{14}$$

ingen eller et endeligt Antal Løsninger, medens Ligningen

$$x^2 - cy^2 = A \tag{15}$$

faar ingen eller uendelig mange Løsninger. Da dette hidrører fra, at vi faa uendelig mange Løsninger for $A = 1$, ville vi nærmere undersøge dette Tilfælde, idet vi forudsætte, at c ikke er et Kvadrattal.

9. Vi ville altsaa nærmere undersøge Ligningen (c positiv)

$$x^2 - cy^2 = 1. \tag{16}$$

Da i denne Ligning x og y samtidig maa vokse eller aftage, kunne vi tale om større og mindre Løsninger, og navnlig ville vi ved den mindste Løsning forstaa den, hvor x og y ere hele

Tal med de mindst mulige numeriske Værdier; ere disse α og β ($\beta \neq 0$), kunne vi da vise, at alle Løsninger bestemmes ved Ligningen

$$x + y\sqrt{c} = (\alpha + \beta\sqrt{c})^n, \tag{17}$$

hvor n gennemløber alle positive, hele Værdier.

Gaa vi ud fra $\alpha + \beta\sqrt{c}$ faa vi, hver Gang vi multiplicere med $\alpha + \beta\sqrt{c}$ en højere Løsning, medens vi gaa tilbage i Rækken af Løsninger, naar vi multiplicere med $\alpha - \beta\sqrt{c}$, da denne Multiplikation er identisk med Divisjon med $\alpha + \beta\sqrt{c}$.

Gaa vi ud fra en vilkaarlig Løsning, og danne vi af denne mindre Løsninger ved successive Divisjoner med $\alpha + \beta\sqrt{c}$, maa vi omsider komme til $\alpha + \beta\sqrt{c}$, da der i modsat Fald maatte gives mindre Løsninger. Den Løsning, vi gik ud fra, maa derfor høre til den ovenfor bestemte Række af Løsninger. Det gælder saaledes ved Ligningens Løsning kun om at finde den laveste Løsning; det kan i Reglen ikke nytte at søge denne ved Forsøg, da, selv for smaa Værdier af c, α og β kunne være meget store; saaledes f. Eks. for $c = 661$, skrives den laveste Værdi af x med 38 Cifre.

Er c et Kvadrattal, er der ingen andre Løsninger end $x = 1$, $y = 0$.

10. Vi ville nu særlig undersøge Ligningen

$$x^2 + y^2 = a, \tag{18}$$

hvor vi, naar vi tale om Antallet af Løsninger, ikke gøre Forskel paa saadanne, som kun ere forskellige ved Fortegnene for x og y eller ved, at disse ere ombyttede; vi vide, at hvis x og y ere indbyrdes primiske, kan a kun indeholde ulige Primfaktorer af Formen $4n + 1$; hvis der derfor i a findes en Primfaktor af Formen $4n + 3$, maa den være fælles Faktor for x og y og findes i a med lige Eksponent, altsaa:

Indeholder a en Primfaktor $4n + 3$ med ulige Eksponent, er Opgaven umulig.

Antag nu

$$a = 2^q.$$

For $q = 1$, have vi kun Løsningen $x = y = 1$, saa med en let forstaaelig Betegnelse

$$(1 + \sqrt{-1})\ (1 \pm \sqrt{-1})\ (1 \pm \sqrt{-1}) \ldots (q \text{ Fakt.}) = (2^q).$$

Nu er imidlertid

$$1 - \sqrt{-1} = -\sqrt{-1}\,(1 + \sqrt{-1}),$$

saa at Ligningen ogsaa kan skrives

$$(19) \qquad (2^q) = (1 + \sqrt{-1})^q,$$

idet en Faktor $(\sqrt{-1})^\alpha$ kun kan gøre, at x og y ombyttes. Altsaa:

Naar a er en Potens af 2, har Ligningen kun een Løsning.

Er $a = p^q$, hvor $p = 4n + 1$, og er

$$\alpha + \beta\sqrt{-1} = (p),$$

faar man

$$(20) \qquad (p^q) = (\alpha + \beta\sqrt{-1})^\mu\,(\alpha - \beta\sqrt{-1})^\nu,\ (\mu + \nu = q)$$

saa at Udtrykket faar $q + 1$ Værdier; af disse ere imidlertid for q ulige to og to kun forskellige ved Fortegnet for $\sqrt{-1}$, medens for q lige den, som svarer til $\mu = \nu = \frac{1}{2}q$, ikke forandres ved Ombytningen; vi faa altsaa henholdsvis $\frac{1}{2}(q + 1)$ eller $\frac{1}{2}(q + 2)$ Løsninger.

Indeholder a andre analoge Primtalpotenser, maa vi multiplicere (20) med de analoge Udtryk. I Resultatet ville da to og to Udtryk kun være forskellige ved Fortegnet for $\sqrt{-1}$, med mindre alle Eksponenterne ere lige, da et af Udtrykkene ikke forandres ved Ombytningen. Altsaa

Er

$$a = 2^q p_1^{q_1} p_2^{q_2} \ldots,$$

hvor Primfaktorerne p ere af Formen $4n + 1$, er Løsningernes Antal

$$\frac{1}{2}(q_1 + 1)(q_2 + 1)\ldots, \tag{21}$$

hvortil maa adderes $^1/_2$, hvis q_1, q_2 alle ere lige.

Dersom vi gøre Forskel paa de Løsninger, hvor blot x og y ere ombyttede, bliver Antallet

$$(q_1 + 1)(q_2 + 1)(q_3 + 1)\ldots,$$

hvortil der skal adderes 1, hvis alle q ere lige, altsaa, hvis a er et Kvadrat eller det dobbelte af et Kvadrat; i det første Tilfælde regne vi her $0 + m^2$ og $m^2 + 0$ for to Løsninger, i det sidste regne vi $m^2 + m^2$ for to Løsninger. Dersom vi derfor fastsætte, at vi kun regne den sidste for een Løsning, og at den ene af de ubekendte ikke maa være Nul, er Løsningernes Antal altid

$$(q_1 + 1)(q_2 + 1)(q_3 + 1)\ldots. \tag{22}$$

Dette Tal angiver netop Antallet af Divisorer i Tallet, naar vi af dette bortfjerne alle Primfaktorer 2 og $4n + 3$. Dette er det samme, som Antallet af Divisorer af Formen $4n + 1$, minus Antallet af Divisorer af Formen $4n + 3$.

11. Enhver Divisor i en Sum af to indbyrdes primiske Kvadrattal, er selv en Sum af to Kvadrattal.

Vi sætte

$$a^2 + b^2 = pq,$$

hvor p er den mindste Primfaktor og antage, at Sætningen er bevist for lavere Værdier af Kvadratsummen; a og b kunne ikke begge være mindre end $\frac{1}{2}p$ og maa derfor ved Divisjon med p kunne give Rester (pos. eller neg.), af hvilke i det mindste den ene er mindre end Dividenden; vi komme derved, idet vi kalde Resterne α og β, til en ny Ligning af Formen

$$\alpha^2 + \beta^2 = mp.$$

Hverken α eller β kan være Nul, og have de en fælles Faktor, maa denne findes i m og tænkes bortdivideret; da nu

$$\alpha^2 + \beta^2 < a^2 + b^2,$$

gælder Sætningen ifølge vor Forudsætning for den ny Ligning, og p er derfor en Sum af to Kvadrater; det samme gælder da ifølge 7 om q, og da $q < a^2 + b^2$, om q's Divisorer, altsaa om $a^2 + b^2$.

12. Ethvert Primtal af Formen $4n+1$ kan skrives som en Sum af to Kvadrattal.

Ifølge Wilsons Sætning gaar Primtallet op i

$$1 \cdot 2 \cdot 3 \cdot 4 \ldots 4n + 1,$$

eller, da de sidste $2n$ Tal i Produktet ere kongruente med de første $2n$ med modsatte Fortegn, i

$$(1 \cdot 2 \cdot 3 \ldots 2n)^2 + 1.$$

Da Primtallet saaledes gaar op i en Sum af to Kvadrater, er det ifølge den forrige Sætning selv en saadan Sum.

Eks. 1. $x^2 + y^2 = 5 \cdot 13^2$.

$2 + \sqrt{-1} = (5)$; $3 + 2\sqrt{-1} = (13)$.

$x + y\sqrt{-1} = (2 + \sqrt{-1})(3 + 2\sqrt{-1})^2$; $x = 2$; $y = 29$.

$x + y\sqrt{-1} = (2 + \sqrt{-1})(3 - 2\sqrt{-1})(3 + 2\sqrt{-1})$;

$x = 26$; $y = 13$.

$x + y\sqrt{-1} = (2 + \sqrt{-1})(3 - 2\sqrt{-1})^2$; $x = 22$; $y = 19$.

Eks. 2. $x^2 + y^2 = 5 \cdot 13^2 \cdot 19^2$.

Løsningerne faas ved at multiplicere de foregaaende med 19.

13. Om Ligningen

$$x^2 + 2y^2 = a \tag{23}$$

vide vi, at hvis x og y ere indbyrdes primiske, maa alle ulige Primfaktorer i a være af en af Formerne $8n + 1$ eller $8n + 3$;

hvis derfor a har Primfaktorer af Formerne $8n+5$ eller $8n+7$, maa disse forekomme med lige Eksponenter og blive fælles for x og y. Altsaa:

Indeholder a Primfaktorer $8n+5$ eller $8n+7$ med ulige Eksponent, er Opgaven umulig.

For $a = 2$ have vi

$$0 + \sqrt{-2} = (2)$$

og derfor

$$(\pm\sqrt{-2})^q = (2^q),$$

som viser, at

Naar a er en Potens af 2, har Opgaven kun een Løsning.

Er $a = p^q$, og have vi

$$\alpha + \beta\sqrt{-2} = (p),$$

hvad der nødvendigvis kræver, at p er af en af Formerne $8n+1$ eller $8n+3$, faa vi

$$p^q = (\alpha + \beta\sqrt{-2})^\mu\,(\alpha - \beta\sqrt{-2})^\nu,\ (\mu + \nu = q),$$

der giver $q+1$ Værdier; har a flere analoge Faktorer, maa vi multiplicere med de analoge Udtryk. Ganske som for $c = -1$ faa vi da Antallet

$$\frac{1}{2}(q_1+1)(q_2+1)\ldots\ldots,$$

hvor vi maa addere $^1/_2$, hvis alle q ere lige Tal.

Saaledes for

$$a = 11 \cdot 17,$$

faa vi

$$(11) = 3 \pm \sqrt{-2};\ (17) = 3 \pm 2\sqrt{-2};$$
$$(187) = (3+\sqrt{-2})(3+2\sqrt{-2}) = 5 + 9\sqrt{-2};$$
$$(3+\sqrt{-2})(3-2\sqrt{-2}) = 13 - 3\sqrt{2},$$

saa at vi faa $^1/_2 \cdot 2 \cdot 2 = 2$ Løsninger, nemlig

$$187 = 5^2 + 2 \cdot 9^2 = 13^2 + 2 \cdot 3^2.$$

For $a = 17^2$ faa vi paa samme Maade

$$(289) = (3 \pm 2\sqrt{-2})^2 = 1 \pm 12\sqrt{-2};$$
$$(3 + 2\sqrt{-2})(3 - 2\sqrt{-2}) = 17,$$

altsaa to Løsninger, hvis y tør være Nul, nemlig

$$289 = 1 + 2 \cdot 12^2 = 17^2.$$

Primfaktorer $8n + 5$ og $8n + 7$ forandre ikke Løsningernes Antal, hvis deres Eksponenter ere lige, men gøre Opgaven umulig, hvis nogen af dem har ulige Eksponent.

14. Enhver Faktor i $x^2 + 2y^2$, hvor x er primisk med $2y$, har samme Form.

Beviset føres ganske som for en Sum af to Kvadrattal.

15. Ethvert Primtal $8n + 1$ eller $8n + 3$ kan skrives som en Sum af et Kvadrat og det dobbelte af et Kvadrat og det kun paa een Maade.

Ethvert saadant Tal maa nemlig findes som Faktor i visse Tal $x^2 + 2y^2$, da Kongruensen

$$x^2 + 2 \equiv 0 \pmod{p}$$

altid har Løsninger.

16. Vi ville endnu undersøge Ligningen

$$x^2 + 3y^2 = a. \tag{24}$$

Hvis a er delelig med 3, kan denne Faktor bortdivideres, uden at Ligningens Form forandres; er a lige maa x og y begge være lige eller begge ulige; i det første Tilfælde kan 4 bortdivideres, uden at Ligningens Form forandres; i det andet kan 4 ogsaa bortdivideres, idet

$$(2n + 1)^2 + 3(2m + 1)^2$$

er delelig med 4; idet vi sætte

$$4 = 1^2 + 3 \cdot 1^2,$$

kan (13) benyttes, og vi faa

$$\frac{(2n+1)^2+3(2m+1)^2}{1^2+3\cdot 1^2}=\alpha^2+3\beta^2,$$

hvor

$$\beta=\frac{2n+1\pm(2m+1)}{4},$$

der maa give en hel Værdi, da af to ulige Tal enten Summen eller Differensen er delelig med 4; til den hele Værdi af β maa svare en hel Værdi af α, og 4 kan saaledes bortdivideres, uden at Ligningens Form forandres. Hvis a er lige, men ikke delelig med 4, er Opgaven umulig.

Vi have vist, at hvis x og $3y$ ere indbyrdes primiske, maa alle Primfaktorer i a være af Formen $6n+1$; hvis derfor a har Primfaktorer af Formen $6n-1$, maa disse findes i x og y og findes i a med lige Eksponent. Idet vi gaa frem som i de foregaaende Tilfælde, faa vi nu:

Naar a er et ulige Tal, hvis Primfaktorer $6n-1$ har lige Eksponenter, medens Primfaktorerne $6n+1$ have Eksponenterne q_1, q_2 . . ., der ikke alle ere lige, har Ligningen

$$x^2+3y^2=a.$$

$$\frac{1}{2}(q_1+1)(q_2+1)\ldots \tag{25}$$

Løsninger:

Tilføje vi Faktoren 4, bliver Løsningernes Antal 3 Gange saa stort, da vi ikke alene faa saadanne ved at multiplicere med $1\pm\sqrt{-3}$, men ogsaa ved at multiplicere med 2.

Saaledes er

$$7=2^2+3\cdot 1^2,$$

men

$$28=1^2+3\cdot 3^2=4^2+3\cdot 2^2=5^2+3\cdot 1^2.$$

Yderligere Tilføjelser af Faktoren 4 forøger ikke Løsningernes Antal, idet man blot skal multiplicere de tidligere Løsninger med Potenser af 4. Grunden hertil ligger i, at

$$(1+\sqrt{-3})^2=-2(1-\sqrt{-3});\ (1+\sqrt{-3})^3=-8.$$

Saaledes faar man den fuldstændige Løsning

$$112 = 2^2 + 3 \cdot 6^2 = 8^2 + 3 \cdot 4^2 = 10^2 + 3 \cdot 2^2.$$

Sætte vi

$$a^2 + 3b^2 = pq,$$

hvor p er den mindste Primfaktor, kunne vi ikke have baade a og b mindre end eller lig $\frac{1}{2}(p-1)$, da deraf vilde følge

$$a^2 + 3b^2 \leqq (p-1)^2,$$

som strider mod, at p er den mindste Primfaktor; vi kunne da gaa frem som tidligere og faa, idet vi betragte 4 som et Primtal:

Alle Divisorer i et Tal $x^2 + 3y^2$, hvor x og $3y$ ere indbyrdes primiske, kunne skrives paa samme Form, og

Ethvert Primtal $6n + 1$ kan skrives paa Formen $x^2 + 3y^2$ og det kun paa een Maade.

17. De her behandlede Former ere specielle Tilfælde af de almindelige kvadratiske Former, men have en særlig historisk Interesse, idet de fleste af de nævnte Sætninger ere fremsatte af *Fermat* og beviste af *Brownker, Euler, Lagrange, Legendre* o. fl., dog ad andre Veje end de her benyttede. Vi ville hertil knytte et Par Sætninger, som ogsaa falde ind under den almindelige Teori, men som vi med de Midler, vi nu have til Raadighed, kunne give simple Beviser for.

Dersom vi i Ligningen

$$x^2 + y^2 = a$$

for x og y indsætte alle hele og positive Tal, for y tillige Nul, faa vi for a alle de Værdier, for hvilke Ligningen har Løsninger, og hver Værdi faas netop saa mange Gange, som der er Løsninger, idet vi regne $m^2 + n^2$ og $n^2 + m^2$ som to Løsninger, naar m og n ere forskellige og ingen af dem er Nul; vi ville nu vise, at alle Værdierne af a, enhver af dem det fundne Antal Gange, kunne faas frem paa en hel anden Maade.

Lad os betragte de to Rækker af Tal

$$1, 2, 3, 4 \ldots,$$
$$1, -3, 5 - 7, 9 \ldots;$$

den første indeholder alle positive, hele Tal, den anden alle ulige Tal dog saaledes, at alle de, der have Formen $4n + 3$ faa Fortegnet $-$; vi multiplicere nu ethvert af Tallene i den ene Række med ethvert af Tallene i den anden Række og ville bevise, at vi derved netop faa alle Tallene a, ethvert af dem det rigtige Antal Gange, idet vi regne, at en Værdi af a med Fortegnet $+$ og den samme Værdi med Fortegnet $-$ hæve hinanden. Det Antal Gange, enhver Værdi af a skal forekomme, er ifølge (22)

$$(q_1 + 1)\ (q_2 + 1)\ (q_3 + 1) \ldots,$$

naar der i a forekommer Primfaktorer $4n + 1$ med Eksponenterne q_1, q_2, $q_3 \ldots$, medens andre Primfaktorer ikke have nogen Indflydelse paa Antallet.

Lad nu a være et ulige Tal, der har mindst en Primfaktor $4n + 3$ med ulige Eksponent. Ifølge (10) har a da lige mange Divisorer $4n + 1$ og $4n + 3$. Lad os nu i den første Række opsøge alle Divisorerne, altsaa lige mange af hver af de to Former. Er a af Formen $4n + 3$, maa det første Sæt Divisorer multipliceres med negative Tal af den anden Række, det andet med positive, omvendt, hvis a er af Formen $4n + 1$; i begge Tilfælde faar man altsaa, at a forekommer Nul Gange, stemmende med, at Ligningen for saadanne a er uden Løsninger.

Har a ingen Primfaktor $4n + 3$, blive alle Produkterne positive, og vi faa derfor a saa mange Gange, som der er Divisorer, stemmende med Antallet af Ligningens Løsninger i dette Tilfælde.

Indeholder a en Primfaktor $4n + 3$ med lige Eksponent, kan den bortkastes; have vi saaledes f. Eks. Faktoren 7^4, finde vi i øverste Række, idet m er en Faktor,

$$m \cdot 7, m \cdot 7^2, m \cdot 7^3, m \cdot 7^4,$$

hvortil svare i nederste Række Tal af Formen

$$n \cdot 7^3, n \cdot 7^2, n \cdot 7, n \cdot 1,$$

der afvekslende ere positive og negative; vi kunne derfor udelade i den første Række alle Divisorer, der indeholde Faktoren $4n + 3$, og Resultatet er saaledes det samme, som om denne Faktor manglede, stemmende med det, vi vide om Ligningens Løsninger i dette Tilfælde.

Indeholder endelig a Faktoren 2^r, kunne vi af den første Række kun benytte Tal, der ere delelige med 2^r; det søgte Antal Gange er derfor det samme, som om denne Faktor manglede. Hermed er Sætningen fuldstændig bevist.

18. Idet vi multiplicere hvert Tal af første Række med hvert Tal af anden Række, danne vi de samme Produkter, som om vi multiplicerede Summen af Tallene i første Række med Summen af Tallene i anden Række; disse Summer ere imidlertid meningsløse, da de danne divergente Rækker. Nu er imidlertid Samlingen af Tallene a identisk med Samlingen af Produkter, vi danne, og denne Identitet maa vedblive at finde Sted, naar vi begge Steder for ethvert Tal sætte en bestemt Funktion af Tallet, og det gælder da om at vælge denne Funktion saaledes, at Summerne af Tallene i begge vore Samlinger give konvergente Rækker. Dette bliver Tilfældet, naar vi for ethvert af Tallene n sætte n^{-s}, hvor s er et vilkaarligt, reelt eller komplekst Tal, hvis reelle Del er positiv og > 1; vi faa saaledes den mærkelige Ligning

$$(26) \qquad \sum \frac{1}{(x^2 + y^2)^s} = (1 + \frac{1}{2^s} + \frac{1}{3^s} \ldots)(1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \ldots),$$

hvor ved Summationen x skal antage alle Værdierne $1, 2, 3 \ldots$, y de samme Værdier og tillige Værdien Nul.

19. Ved at gaa frem paa samme Maade faar man

$$(27) \sum \frac{1}{(x^2 + 2y^2)^s} = (1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots)(1 + \frac{1}{3^s} - \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} - \ldots),$$

hvor x og y ere alle negative Tal, x tillige Nul og alle positive Tal, y tillige Nul. I den anden Parentes ere de Led negative, hvor Tallet i Nævneren har Formen $8n + 5$ eller $8n + 7$.

ANDET KAPITEL.

I. DE KVADRATISKE RESTERS SUM OG FORDELING.

20. Idet vi ved p forstaa et ulige Primtal, ved r og i henholdsvis Rester og Ikkerester, have vi for Mod. p:

$$\Sigma r \equiv 1^2 + 2^2 + 3^2 + \ldots + \left(\frac{p-1}{2}\right)^2 = \frac{1}{24} p\,(p^2 - 1),$$

$$\Sigma r + \Sigma i \equiv 1 + 2 + 3 + \ldots (p-1) = \frac{1}{2} p\,(p-1).$$

Man slutter heraf $(p > 3)$

$$(28) \qquad \Sigma r = \alpha p;\ \Sigma i = \beta p;\ \alpha + \beta = \frac{1}{2}(p-1),$$

hvor α og β ere hele Tal.

For $p = 4n + 1$ er -1 *R.*, saa at Rester og Ikkerester parvis have Summen p og følgelig

$$(29) \qquad \alpha = \beta = \frac{1}{4}(p-1).$$

For $p = 4n + 3$ ere α og β forskellige, det ene lige, det andet ulige.

Vi ville finde, at Tallene α og β i det følgende spille en stor Rolle, og det er i Virkeligheden disse Tal, der have ført Forf. ind paa mange af de følgende Undersøgelser. Vi ville her gøre den Bemærkning, at det ofte er vanskeligt at sige, hvad man skal forstaa ved en talteoretisk Opgaves Løsning; her kan man jo finde α ved Addition af Resterne; man kan tælle de ulige Rester og derved afgøre, om det er α eller β, der er ulige, men disse Metoder ere praktisk uanvendelige for store Primtal. Kan man nu finde Formler eller Algoritmer, der i væsentlig Grad lette Arbejdet? Vi træffe her meget vanskelige Opgaver. Ja selv en saa simpel Sætning som den, at β for $p = 4n + 3$ altid er større end α, er det kun lykkedes at bevise ad en meget indirekte Vej.

21. Før vi gaa videre, ville vi benytte det fundne Udtryk for Resternes Sum til at udvide en fra Talteorien bekendt Sætning, nemlig den, at Summen af Produkterne af $p-2$ og $p-2$ af Tallene, mindre end p, er delelig med p; vi kunne nemlig vise, at denne Sum er delelig med p^2. Summen kan skrives

$$\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}\cdots+\frac{1}{p-1}\right)(p-1)!$$

eller, idet vi addere første og sidste, næstførste og næstsidste Brøk o. s. v. og bortdividere Faktoren p

$$\left(\frac{1}{1\,.\,(p-1)}+\frac{1}{2\,(p-2)}+\cdots\frac{1}{\alpha\,(p-\alpha)}\cdots+\frac{1}{\frac{1}{4}\,(p^2-1)}\right)(p-1)!$$

eller, naar vi bortkaste de med p delelige Led i Nævneren og forandre Fortegn

$$\left(\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots\frac{1}{\frac{1}{4}\,(p-1)^2}\right)(p-1)!$$

Her ere Nævnerne kongruente med alle Resterne, og da 1 er $R.$, gælder det samme om Brøkerne, og da Resternes Sum er delelig med p, er Sætningen bevist.

22. For at beregne α og β, kunne vi gaa følgende Vej: Vi have

$$\frac{1}{24}p\,(p^2-1)=mp+\Sigma r=(m+\alpha)\,p,$$

hvor m er Summen af de ufuldstændige Kvotienter, som man faar, naar man dividerer de $\frac{1}{2}(p-1)$ første Kvadrattal med p. Disse Kvotienter ere Nul for de Kvadrattal, der ere mindre end p, 1 for Kvadrattallene mellem p og $2p$, i Antal $(\sqrt{2p})-(\sqrt{p})$*), 2 for dem mellem $2p$ og $3p$, i Antal $(\sqrt{3p})-(\sqrt{2p})$ o. s. v. Da nu $\frac{1}{4}(p-1)^2$ ligger mellem $\frac{1}{4}(p-1)p$ og $\frac{1}{4}(p-5)p$ for $p=4n+1$ og mellem $\frac{1}{4}(p-3)p$ og $\frac{1}{4}(p+1)p$ for $p=4n+3$, faar man i de to Tilfælde

$$m=1\,.\,[(\sqrt{2p})-(\sqrt{p})]+2\,.\,[(\sqrt{3p})-(\sqrt{2p})]\,.\,.\,.\,.$$

*) $(\sqrt{n})$ betyder det største hele Tal, mindre end $\sqrt{n}$.

$$+\frac{p-5}{4}\left[\left(\sqrt{\frac{p-1}{4}\cdot p}\right)-\left(\sqrt{\frac{p-5}{4}\cdot p}\right)\right]$$

$$=-\left[(\sqrt{p})+(\sqrt{2p})+(\sqrt{3p})\ldots\ldots+\left(\sqrt{\frac{p-5}{4}\cdot p}\right)\right]+\frac{1}{8}(p-1)(p-5)$$

og

$$m=-\left[(\sqrt{p})+(\sqrt{2p})+(\sqrt{3p})\ldots.+\left(\sqrt{\frac{p-3}{4}\cdot p}\right)\right]+\frac{1}{8}(p-1)(p-3),$$

hvoraf, ved at indsætte i Udtrykket ovenfor, henholdsvis

$$(30)\quad \alpha=(\sqrt{p})+(\sqrt{2p})+\ldots\ldots+\left(\sqrt{\frac{p-5}{4}\cdot p}\right)-\frac{1}{12}(p-1)(p-8)$$

$$(p=4n+1)$$

og

$$(31)\quad \alpha=(\sqrt{p})+(\sqrt{2p})+\ldots\ldots+\left(\sqrt{\frac{p-3}{4}\cdot p}\right)-\frac{1}{12}(p-1)(p-5)$$

$$(p=4n+3).$$

Vi vide nu imidlertid, at vi i det første Tilfælde have $\alpha=\frac{1}{4}(p-1)$ og faa derved den mærkelige Formel

$$(\sqrt{p})+(\sqrt{2p})+(\sqrt{3p})+\ldots\ldots+\left(\sqrt{\frac{p-5}{4}\cdot p}\right)=\frac{1}{12}(p-1)(p-5)^{*})$$

$$(p=4n+1).$$

23. For $p=4n+3$ kan Beregningen lettes noget, idet den kan udføres direkte for de sidste Led. Sættes

$$\sqrt{(p-4m-3)\cdot p}=p-2(m+1),$$

bliver Resten

$$p-4(m+1)^2,$$

der er positiv og ikke for stor for

$$m=0,1,2,\quad (\sqrt{\tfrac{1}{4}p})-1.$$

---

*) En analog Formel er følgende:
$(\sqrt{1})+(\sqrt{2})+\ldots\ldots+(\sqrt{n^2-1})=1\cdot(2^2-1^2)+2(3^2-2^2)+(n-1)(n^2-(n-1)^2)=\frac{1}{6}n(n-1)(4n+1)$.

De tilsvarende Led faa Summen

$$s = \frac{1}{2}[p - 2 - (\sqrt{\tfrac{1}{4}p})](\sqrt{\tfrac{1}{4}p}), \tag{32}$$

saa at

$$\alpha = (\sqrt{p}) + (\sqrt{2p}) + \ldots\ldots + \left(\sqrt{\tfrac{1}{4}p\,(p - 3 - 4\,(\sqrt{\tfrac{1}{4}p})}\right) + s - \frac{1}{12}(p-1)(p-5). \tag{33}$$

For f. Eks. $p = 179$ stille Regningerne sig saaledes:

mp	$(\sqrt{mp})$	mp	$(\sqrt{mp})$	mp	$(\sqrt{mp})$	mp	$(\sqrt{mp})$
179	13	1969	44	3759	61	5549	74
358	18	2148	46	3938	62	5728	75
537	23	2327	48	4117	64	5907	76
716	26	2506	50	4296	65	6086	78
895	29	2685	51	4475	66	6265	79
1074	32	2864	53	4654	68	6444	80
1253	35	3043	55	4833	69	6623	81
1432	37	3222	56	5012	70	6802	82
1611	40	3401	58	5191	72		
1790	42	3580	59	5370	73		

$\Sigma(\sqrt{mp}) = 2110$; $s = 513$; $\alpha = 2623 - 2581 = 42$; $\beta = 47$.

I følgende Tabel findes Løsningerne for de første Primtal $4n + 3$:

p	α	β	p	α	β	p	α	β	p	α	β	p	α	β
7	1	2	43	10	11	79	17	22	131	30	35	179	42	47
11	2	3	47	9	14	83	19	22	139	33	36	191	41	54
19	4	5	59	13	16	103	23	28	151	34	41	199	45	54
23	4	7	67	16	17	107	25	28	163	40	41			
31	6	9	71	14	21	127	29	34	167	36	47			

II. VARIATIONER OG PERMANENSER.

24. Naar to paa hinanden følgende Tal i Talrækken begge ere *R.* eller begge *I.*, ville vi sige, at de danne en Permanens, i modsat Fald en Variation. Det første Tal i Variationerne og i Permanenserne bestemmes henholdsvis ved Kongruenserne (mod. p).

$$(34) \quad (x+1)^{\frac{1}{2}(p-1)} + x^{\frac{1}{2}(p-1)} \equiv 0 \text{ og } (x+1)^{\frac{1}{2}(p-1)} - x^{\frac{1}{2}(p-1)} \equiv 0.$$

Da begge disse Kongruenser høre til dem, der have saa mange Rødder, som Graden angiver, har man altsaa:

I Talrækken $1, 2, 3 \ldots p-1$ er der $\frac{1}{2}(p-1)$ Variationer og $\frac{1}{2}(p-3)$ Permanenser.

Det samme gælder om Rækken (mod. p)

$$k, 2k, 3k, (p-1)k; \; k = 1, 2, 3 \ldots p-1,$$

hvor de bestemmende Kongruenser dannes af dem ovenfor ved at sætte $x+k$ for $x+1$; det er ogsaa indlysende, at hvis to Tal ere af samme eller forskellig Natur, og man multiplicerer dem begge med k, maa man atter faa to Tal af samme eller forskellig Natur.

Saaledes faa vi f. Eks. for $p = 31$, $k = 1$

$$\underset{\cdot}{2}\ 3\ \underset{\cdot}{5}\ 6\ \underset{\cdot}{10}\ 13\ \underset{\cdot}{14}\ 15\ \underset{\cdot}{16}\ 17\ \underset{\cdot}{20}\ 24\ \underset{\cdot}{25}\ 27\ \underset{\cdot}{28}$$

$$\underset{\cdot}{1}\ \underset{\cdot}{4}\ \underset{\cdot}{7}\ \underset{\cdot}{8}\ \underset{\cdot}{9}\ 11\ 12\ \underset{\cdot}{18}\ \underset{\cdot}{19}\ 21\ 22\ 23\ 26\ 29$$

hvor de mærkede Tal ere *R.*, de andre *I.* Ombytte vi i en af Kongruenserne x med $p-1-x$, faa vi den samme Kongruens igen, saa at Rødderne parvis have Summen $p-1$, dog Tallet $\frac{1}{2}(p-1)$ undtaget. I den Række Tal, der bestemmer Variationerne, findes afvekslende en *R.* og en *I.*, thi hvis det første Tal i en Variation er en *R.*, maa det første Tal i den næste Variation være en *I.* o. s. v.

For $p = 4n+3$ ere to parrede Tal i den øverste Række af samme Natur, i den nederste af modsat Natur, omvendt for $p = 4n+1$.

Er nemlig for $p = 4n + 3$ $a + b = p - 1$, da er $a + 1 + b = p$, altsaa $a + 1$ og b af forskellig Natur (da -1 er I.) Nu er imidlertid i øverste Række a og $a + 1$ af forskellig Natur, i nederste af samme Natur. Paa lignende Maade bevises Sætningen for $p = 4n + 1$.

De parrede Rødder bestemmes ved Ligningen

$$x^2 + x + y \equiv 0, \text{ (mod. } p),$$

hvor y er R. eller I., eftersom Rødderne ere af samme eller forskellig Natur; idet Kongruensen skrives

$$(2x + 1)^2 \equiv 1 - 4y,$$

ser man, at $1 - 4y$ maa være R.

25. Vore Sætninger om Permanenser og Variationer give en Bestemmelse af Resterne, som er uafhængig af deres aritmetiske Natur. Man kan f. Eks. stille følgende Opgave:

Del en Cirkelperiferi i p lige store Dele og forbind Delingspunkterne, saa at man faar alle egentlige og uegentlige regulære p-Kanter; mærk nu en af Vinkelspidserne med sort og de øvrige, Halvdelen med blaat og Halvdelen med rødt; dette skal være gjort saaledes, at man, naar man, ud fra sort, gennemløber en af Polygonernes Perimeter, faar $\frac{1}{2}(p - 3)$ Permanenser ($R - R$ og $B - B$) og $\frac{1}{2}(p - 1)$ Variationer ($R - B$ og $B - R$). Kender man Resterne, kan dette gøres; om der er andre Løsninger, har jeg ikke undersøgt. Maaske bør der tilføjes, at Kvadrattallene skulle have samme Farve.

26. Om Resternes Fordeling kan man ikke sige meget i Almindelighed, da den er i høj Grad afhængig af Primtallets Natur; vi ville derfor specialisere og derved navnlig betragte Primtal af Formen $4n + 3$, da det særlig er disse, der have Betydning for vore følgende Undersøgelser. Om Primtal af Formen $4n + 1$, altsaa saadanne, hvor -1 er R., vide vi, at Rester og Ikkerester fordele sig symmetrisk i Tallenes første og anden Halvdel.

$-1 = I.\ \ p = 4n + 3.$

27. Vi forudsætte altsaa nu, at -1 er $I.$, altsaa at Primtallet har Formen $4n + 3$. Vi betegne Antallene af Rester af Formerne $4n$, $4n + 1$, $4n + 2$ og $4n + 3$ henholdsvis ved r_0, r_1, r_2 og r_3, der derved ogsaa komme til at betegne Resternes Antal henholdsvis i Tallenes første, anden, tredje og fjerde Fjerdedel, det vil sige i de fire Rækker Tal

$$1, 2, 3, \ldots \frac{1}{4}(p-3);\ \frac{1}{4}(p+1)\ldots\frac{1}{2}(p-1);$$

$$\frac{1}{2}(p+1)\ldots\frac{1}{4}(3p-1);\ \frac{1}{4}(3p+3)\ldots p-1.$$

Lad os nu til hvert Tal i de fire Rækker addere henholdsvis 0, p, $2p$ og $3p$ og derpaa dividere alle de udkomne Tal med 4; vi faa da alle Resterne, saa at

$$4\Sigma r = \Sigma r + (r_1 + 2r_2 + 3r_3)p$$

eller

$$3\alpha = r_1 + 2r_2 + 3r_3 \tag{35}$$

og, idet man behandler Ikkeresterne paa samme Maade, og erindrer, at

$$\begin{gathered} i_3 = r_0,\ i_2 = r_1,\ i_1 = r_2,\ i_0 = r_3 \\ 3\beta = 3r_0 + 2r_1 + r_2. \end{gathered} \tag{36}$$

Ved Subtraktion udledes af de to Ligninger, at

$$r_1 - r_2 = i_2 - i_1 = r_1 - i_1 = i_2 - r_1$$

er delelig med 3 altsaa:

I Tallenes anden og i deres tredje Fjerdedel er Forskellen mellem Resternes og Ikkeresternes Antal delelig med 3.

Af andre Formler ville vi nævne

$$\Sigma i^2 - \Sigma r^2 = \Sigma(p-r)^2 - \Sigma r^2 = p\,\Sigma(p-2r) = (\beta-\alpha)p^2 \tag{37}$$

og, da

$$\Sigma i^2 + \Sigma r^2 = \frac{1}{6}(p-1)p(2p-1)$$

$$\Sigma r^2 = \alpha p^2 - \frac{1}{12}(p-1)p(p+1);\ \Sigma i^2 = \beta p^2 - \frac{1}{12}(p-1)p)(p+1), \tag{38}$$

hvoraf, idet i og r ere sammenhørende ($i + r = p$),

$$\Sigma ir = \frac{1}{12}(p-1)\,p\,(p+1);$$

$$\Sigma r_i r_j = \frac{1}{2}\alpha(\alpha-1) + \frac{1}{24}(p-1)\,p\,(p+1).$$

$$2 = R.\quad p = 8n - 1.$$

28. Ved Multiplikation af Σr med 2, faa vi Σr og p saa mange Gange, som der er Rester $> \frac{1}{2}(p-1)$. Altsaa er

$$2\alpha p = \alpha p + (r_2 + r_3)\,p,$$

hvoraf

$$\alpha = r_2 + r_3 = i_1 + i_0$$

eller

Blandt Tallene $\leqq \frac{1}{2}(p-1)$ er der β *R.* og α *I.*

Blandt Tallene $> \frac{1}{2}(p-1)$ er der α *R.* og β *I.*

Idet vi addere p til hver ulige *R.* (i Antal r_u) og dividere med 2, faa vi alle Resterne eller

$$\Sigma r + r_u p = 2\,\Sigma r;\ r_u = \alpha,$$

altsaa:

Der er α ulige, β lige Rester.

Vi have saaledes $r_1 + r_3 = \alpha$ og fandt ovenfor $r_2 + r_3 = \alpha$; altsaa er

$$r_1 = r_2$$

eller:

Der er lige mange Rester af Formerne $4n + 1$ og $4n + 2$ eller i Tallenes anden og tredje Fjerdedel.

Da nu en *R.* i den anden Fjerdedel svarer til en *I.* i den tredje Fjerdedel og omvendt, følger heraf:

I den anden saa vel som i den tredje Fjerdedel er der $\frac{1}{8}(p+1)$ *R.* og $\frac{1}{8}(p+1)$ *I.*,

hvoraf atter følger:

Af de lige Tal $> \frac{1}{2}(p-1)$ er $\frac{1}{8}(p+1)$ *R.* og lige saa mange *I.*

Af de ulige Tal $\gtreqless \frac{1}{2}(p-1)$ ere $\frac{1}{8}(p+1)$ *R.* og lige saa mange *I.*

Af de fundne Resultater og de ovenfor fundne Udtryk for 3α og 3β faar man nu

$$r_1 = r_2 = \frac{1}{8}(p+1);\ r_0 = \frac{1}{8}(3p-5) - \alpha;\ r_3 = \alpha - \frac{1}{8}(p+1),$$

der atter give

$$r_0 - i_0 = r_0 - r_3 = \frac{1}{8}(3p-5) + \frac{1}{8}(p+1) - 2\alpha = \frac{1}{2}(p-1) - 2\alpha = \beta - \alpha$$

eller:

I Tallenes første Fjerdedel er Forskellen mellem Antallet af Rester og Antallet af Ikkerester lig $\beta - \alpha$.

Trækker man hver af de α *R.*, større end $\frac{1}{2}(p-1)$ fra p, faar man de α *I.* $\gtreqless \frac{1}{2}(p-1)$; disses Sum er derfor αp minus Summen af Resterne større end $\frac{1}{2}(p-1)$ eller, da αp er Summen af alle Resterne:

I den første Halvdel af Tallene er Summen af Resterne lig Summen af Ikkeresterne, nemlig lig $\frac{1}{16}(p^2-1)$.

Vi have set, at $\beta - \alpha$ er Antallet af *R.* minus Antallet af *I.* i Tallenes første Halvdel; nu er imidlertid, da -1 er *I.* og 2 er *R.*, Tallene k og $\frac{1}{2}(p-k)$ af modsat Natur, saa at de kunne borttages, naar man søger $\beta - \alpha$; man borttager altsaa 1 og $\frac{1}{2}(p-1)$, 3 og $\frac{1}{2}(p-3)\ldots$, $2m-1$ og $\frac{1}{2}(p+1) - m$, hvor $\frac{1}{2}(p+1) - m > 2m - 1$ eller $m < \frac{1}{6}(p+3)$. Tilbage bliver

saaledes kun de lige Tal op til $2m+1$ eller, da 2 er *R.*, Tallene $1, 2, 3 \ldots$, hvor det sidste Tal bliver $\frac{1}{6}(p+1)$ for $p = 24n-1$, $\frac{1}{6}(p-1)$ for $p = 24n+7$.

Eks. $p = 127$; $\frac{1}{6}(p-1) = 21$. Mindre end og lig 21 findes 8 *I.*, nemlig 3, 5, 6, 7, 10, 12, 14, 20 og 13 *R.* Man har altsaa $\beta - \alpha = 5$, hvoraf $\alpha = 29$; $\beta = 34$.

Idet vi betragte Resterne af Formerne $8n$, $8n+1$, $8n+2 \ldots 8n+7$, faa vi med analoge Betegnelser

$$\varrho_1 = \varrho_2 = \varrho_4;\ \varrho_3 = \varrho_5 = \varrho_6;\ \varrho_0 + \varrho_7 = \frac{1}{8}(p-7);$$
$$\varrho_1 + \varrho_6 = \frac{1}{8}(p+1);\ \varrho_0 + \varrho_1 = \beta - \frac{1}{8}(p+1). \tag{39}$$

Lad lige og ulige *R.* og *I.* betegnes ved Mærkerne l og u. Multipliceres alle *I.* med 2, kunne vi skrive ethvert af Produkterne, større end p, som en ulige *I.* plus p; vi faa saaledes:

$$\Sigma(2i)^n = \Sigma i_l^n + \Sigma(p+i_u)^n,$$

hvoraf, da

$$\Sigma i_l^n + \Sigma i_u^n = \Sigma i^n,$$

$$(2^n-1)\,\Sigma i^n = \beta p^n + \frac{n}{1}p^{n-1}\,\Sigma i_u + \frac{n(n-1)}{1\cdot 2}p^{n-2}\,\Sigma i_u^2 + \ldots + \frac{n}{1}p\,\Sigma i_u^{n-1}$$

og paa lignende Maade:

$$(2^n-1)\,\Sigma r^n = \alpha p^n + \frac{n}{1}p^{n-1}\,\Sigma r_u + \frac{n(n-1)}{1\cdot 2}p^{n-2}\,\Sigma r_u^2 + \ldots + \frac{n}{1}p\,\Sigma r_u^{n-1}$$

altsaa, da $\Sigma(i_u - r_u) = (\beta - \alpha)p$,

$$(2^n-1)\,\Sigma(i^n - r^n) = (n+1)(\beta-\alpha)p^n + \frac{n(n-1)}{1\cdot 2}p^{n-2}\,\Sigma(i_u^2 - r_u^2) + \ldots$$
$$+ \frac{n}{1}p\,\Sigma(i_u^{n-1} - r_u^{n-1}).$$

Ligningerne vise, at

Tallet p gaar op i Σi^n og i Σr^n, hvis det ikke gaar op i $2^n - 1$,

og for $n = p$, da $2^p - 1 \equiv 1 \pmod{p}$,

$$p^2 \text{ gaar op i } \Sigma i^p \text{ og i } \Sigma r^p,$$

og da Antallet af i_u og og r_u er henholdsvis β og α

$$\Sigma i^p : p^2 \equiv \beta \pmod{p}; \quad \Sigma r^p : p^2 \equiv \alpha \pmod{p}.$$

For $n = 3$ faa vi

$$7\,\Sigma(i^3 - r^3) = 4(\beta - \alpha)\,p^3 + 3\,p\,\Sigma(i_u^2 - r_u^2)$$

eller, da

$$(\beta - \alpha)\,p^2 = \Sigma(i^2 - r^2) = \Sigma(i_u^2 - r_u^2) + \Sigma(i_l^2 - r_l^2),$$
$$7\,\Sigma(i^3 - r^3) = 7(\beta - \alpha)\,p^3 - 3\,p\,\Sigma(i_l^2 - r_l^2),$$

der viser, at naar p ikke er 7, gaar 7 op i $\Sigma(i_l^2 - r_l^2)$ eller i $\Sigma(i^2 - r^2)$, hvor i og $r \leqq \frac{1}{2}(p-1)$.

2 = *I.* $p = 8n + 3$.

29. Ved Multiplikation med 2 faar man

$$2\,\Sigma r = \Sigma i + m_1 p; \quad 2\,\Sigma i = \Sigma r + m_2 p,$$

hvor m_1 og m_2 betyder Antallene af *R.* og *I.* større end $\frac{1}{2}(p-1)$ eller Antallene af *I.* og *R.* lig eller mindre end $\frac{1}{2}(p-1)$; heraf faas

$$3\,\Sigma r = (m_2 + 2m_1)\,p; \quad 3\,\Sigma i = (m_1 + 2m_2)\,p,$$

altsaa:

$$3(\beta - \alpha) = m_2 - m_1, \tag{40}$$

der viser, at:

Antallet af Rester minus Antallet af Ikkerester i Tallenes første Halvdel er delelig med et ulige Multiplum af 3.

Af Ligningerne ovenfor finder man

$$m_1 = 3\alpha - \frac{1}{2}(p-1); \quad m_2 = 3\beta - \frac{1}{2}(p-1).$$

Idet Bogstaverne have den samme Betydning som tidligere, finder man

$$(41)\quad r_0=r_3=\frac{1}{8}(p-3);\ r_1=\frac{1}{8}(7p-5)-3\alpha;\ r_2=3\alpha-\frac{1}{2}(p-1).$$

Heraf findes

Antallet af ulige Rester er $p-1-3\alpha$, af lige Rester $3\alpha-\frac{1}{2}(p-1)$.

De r_3 Rester af Formen $4n+3$ give, subtraherede fra p, r_3 Ikkerester af Formen $4n$, og naar disse divideres med 4, de r_3 *I.*, som ere $\leqq\frac{1}{4}(p-3)$, men heraf følger, da vi have $r_3=r_0$

I den første Fjerdedel af Tallene er der lige mange *R.* og *I.*

Vi have

$$\alpha p=\Sigma r+\Sigma(p-i)\ (r \text{ og } i\leqq\tfrac{1}{2}(p-1))$$
$$=\Sigma r-\Sigma i+(2\alpha-\beta)p,$$

hvoraf for den første Halvdel af Tallene

$$\Sigma r-\Sigma i=(\beta-\alpha)p.$$

$2=R.;\ 3=R.;\ p=24n-1.$

30. Forstaa vi ved a_0, a_1, a_2 Resterne af Formerne $3n$, $3n+1$ og $3n+2$, faa vi, naar vi gaa frem som tidligere,

$$2\alpha=a_1+2a_2;\ 2\beta=a_1+2a_0$$

og, hvis vi ved $b_0, b_1 \ldots b_5$ forstaa Resterne af Formerne $6n$, $6n+1 \ldots 6n+5$

$$5\alpha=b_1+2b_2+3b_3+4b_4+5b_5;\ 5\beta=5b_0+4b_1+3b_2+2b_3+b_4$$
$$2\alpha=a_1+2a_2=b_1+b_4+2b_2+2b_5;\ 2\beta=a_1+2a_0=b_1+b_4+2b_0+2b_3.$$

Herved findes

$$(42)\quad b_1=b_2=b_3=b_4=\frac{1}{12}(p+1);\ b_0+b_5=\frac{1}{6}(p-5);\ b_0=\frac{1}{3}(p-2)-\alpha.$$

Vi behøve saaledes, for at finde α, kun at undersøge den første Sjettedel af Tallene; vi have tidligere ad en anden Vej vist, at dette overhovedet gælder, naar 2 er *R*. ($p = 8n - 1$).

III. OM PRODUKTET AF DE ULIGE TAL, MINDRE END p.

31. Sætte vi

(43) $$1 . 3 . 5 \ldots (p-2) \equiv x \pmod{p},$$

bliver $$2 . 4 . 6 \ldots (p-1) \equiv (-1)^{\frac{1}{2}(p-1)} x,$$

altsaa $$1 . 2 . 3 \ldots (p-1) \equiv (-1)^{\frac{1}{2}(p-1)} . x^2,$$

hvorved, ifølge Wilsons Sætning

(44) $$x^2 \equiv (-1)^{\frac{p+1}{2}}.$$

Er nu p af Formen $4n + 1$, have vi $x^2 \equiv -1$, der giver to Løsninger, som ere forskellige for forskellige Primtal; større Interesse har Tilfældet $p = 4n + 3$, da vi faa $x = \pm 1$, altsaa:

$$1 . 3 . 5 \ldots (p-2) \equiv \pm 1 \pmod{p = 4n + 3},$$

og her frembyder sig da naturligt Spørgsmaalet om, for hvilke Primtal man faar $+1$, og for hvilke man faar -1; da -1 er *I*. kan Spørgsmaalet ogsaa stilles saaledes:

For hvilke Primtal $4n + 3$ findes der et lige og for hvilke et ulige Antal ulige Ikkerester?

eller under en anden Form, da Ikkeresternes Sum er βp:

For hvilke Primtal $4n + 3$ er β et lige, for hvilke et ulige Tal?

32. I Stedet for de ulige Tal, kan man betragte den første Halvdel af Tallene; den anden Kongruens ovenfor kan nemlig skrives

$$2^{\frac{1}{2}(p-1)} . 1 . 2 . 3 \ldots \frac{p-1}{2} \equiv (-1)^{\frac{1}{2}(p-1)} x \equiv -x \pmod{p = 4n + 3}$$

eller

$$(45) \qquad 1 \cdot 2 \cdot 3 \ldots \frac{1}{2}(p-1) \equiv \mp x \pmod{p = 4n+3}$$

øverste Fortegn, hvis 2 er *R.*, nederste, hvis 2 er *I.*

Af de Værdier, vi have fundet for α og β, faar man nu

$p =$ 3 7 11 19 23 31 43 47 59 67 71 79 83 103
$x = +1 +1 -1 -1 -1 -1 -1 +1 +1 -1 -1 +1 +1 +1$
107 127 131 139 151 163 167 179 191 199.
$+1 +1 -1 +1 -1 -1 -1 -1 +1 +1.$

33. Vi have angivet forskellige Metoder til Beregning af Tallene α og β og ville senere træffe flere andre; af disse er ingen saa simpel, at den kan sammenlignes med vor Bestemmelse af det Legendre'ske Symbol. For Primtal af Formen $8n-1$, er den simpleste Metode maaske den at undersøge den første Sjettedel af Tallene. Ved den Opgave, som her foreligger, skulle vi kun afgøre, om α eller β er lige eller ulige; men uagtet vi i det følgende ville træffe disse Tal paa mange forskellige Omraader, synes intet af disse at føre til væsentlige Lettelser ved Opgavens Løsning. Vi ere her ved en af de Opgaver, som Talteorien saa ofte byder os, nemlig saadanne, hvor der ved Svaret kun er to Ting at vælge imellem, saasom større eller mindre, plus eller minus, lige eller ulige o. s. v., og som trods deres tilsyneladende Simpelhed vise sig at kræve de mest dybtgaaende Undersøgelser og ofte endnu staa uløste.

IV. PERIODISK UDVIKLING AF $\frac{1}{p}$.

34. Lad p være et Primtal og t høre til Eksponenten $\frac{1}{2}(p-1)$.

For at udvikle $\frac{1}{p}$ i t-Talsystemet danne vi da Ligningerne

$$1 = 0 \cdot p + 1,$$
$$t \cdot 1 = a_0 \cdot p + r_1,$$
$$t \cdot r_1 = a_1 \cdot p + r_2,$$
$$\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots$$

$$t \cdot r_k = a_k \cdot p + r_{k+1},$$
$$t \cdot r_{k+1} = a_{k+1} \cdot p + r_{k+2},$$
$$\ldots\ldots\ldots\ldots,$$

hvor vi, efter at have fundet de $\frac{1}{2}(p-1)$ Cifre i Perioden

$$a_0,\ a_1,\ a_2 \ldots$$

atter faa Resten 1. Resterne $1, r_1, r_2 \ldots$ ere alle forskellige, og da t hører til Eksponenten $\frac{1}{2}(p-1)$ og derfor er $R.$, ere alle Størrelserne r kvadratiske Rester for p, og vi have i dem alle Resterne, da de alle ere forskellige og i Antal $\frac{1}{2}(p-1)$. Dersom vi addere alle Ligningerne, kunne vi trække ethvert r fra det første Led i den næste Ligning og faa det da der multipliceret med $t-1$; da nu Resternes Sum er αp, faa vi paa venstre Side Summen $(t-1)\alpha p$, medens vi paa højre Side faa p Gange Summen af de $\frac{1}{2}(p-1)$ Cifre a. Følgelig er

$$(t-1)\alpha = \text{Tværsum af Perioden.}$$

Er specielt $t = 2$, bliver α Tværsummen af Perioden, og da denne kun indeholder Cifrene 0 og 1 har man:

Dersom 2 hører til Eksponenten $\frac{1}{2}(p-1)$, vil Perioden af $\frac{1}{p}$ udviklet i Totalsystemet have α Cifre 1 og β Cifre 0.

Vi ville nu give nogle Eksempler:

$p = 11;\ t = 4;\ \frac{1}{11} = 0{,}01131\ldots\quad T = 6;\ \alpha = 2,\ \beta = 3.$

$p = 19;\ t = 4;\ \frac{1}{19} = 0{,}003113211\ldots\quad T = 12;\ \alpha = 4;\ \beta = 5.$

$p = 23;\ t = 2;\ \frac{1}{23} = 0{,}00001011001\ldots\quad T = \alpha = 4;\ \beta = 7.$

$p = 47;\ t = 2;\ \frac{1}{47} = 0{,}000001010111001001100 1\ldots\quad T = \alpha = 9;\ \beta = 14.$

$p = 71;\ t = 2;\ \frac{1}{71} = 0{,}000000111001101100001010110100100 1 \ldots$
$\alpha = 14;\ \beta = 21.$

$p = 79;\ t = 2;\ \frac{1}{79} = 0{,}000000110011110110010001110100101010001$
$\ldots\ \alpha = 17;\ \beta = 22.$

$p = 167;\ t = 2;\ \frac{1}{167} = 0{,}000000011000100001101110010111111000 01$
$010101110110000010010011001010010110001 1$
$101001 \ldots\ \alpha = 36;\ \beta = 47.$

35. For $p = 8n - 1;\ t = 2$ antage vi, at vi ved en af Divisjonerne have faaet en Rest, der ligger i Tallenes første Fjerdedel; ved Multiplikation med 2 faa vi da en Rest, der ligger i Tallenes første Halvdel og ved næste Multiplikation en Rest, mindre end p; vi faa altsaa i Perioden Permanensen 00; paa samme Maade se vi, at hvis vi have en Rest henholdsvis i den anden, tredje og sidste Fjerdedel, faa vi i Perioden henholdsvis Variationerne 01 og 10 og Permanensen 11; altsaa forekommer i Perioden 00, 01, 10 og 11 henholdsvis r_0, r_1, $r_2 - 1$*) og r_3 Gange.

Ifølge de tidligere fundne Værdier af disse Størrelser have vi altsaa:

Perioden har $\frac{1}{4}(p-3)$ Variationer, nemlig $\frac{1}{8}(p+1)$ Gange 01 og $\frac{1}{8}(p-7)$ Gange 10. Perioden har $\frac{1}{4}(p-3)$ Permanenser, nemlig 00 og 11 henholdsvis $\frac{1}{8}(3p-5) - \alpha$ og $\alpha - \frac{1}{8}(p+1)$ Gange.

Periodens Cifre findes lettest i omvendt Orden, idet man for hver Regning finder et Ettal med de forangaaende Nuller,

---

*) 1 er subtraheret, da vi ikke medregne Variationen 10, som dannes af det sidste Ciffer i Perioden og det første Ciffer i den næste Periode.

saa at der i alt bliver α Regninger; disse skrives bedst, som Eksemplet viser:

$p=79$	$1+79$	16
	5	4
	21	4
	25	8
	13	4
	23	2
	51	2
	65	16
	9	8
	11	2
	45	4
	31	2
	55	2
	67	2
	73	8
	19	2
	49	128
$\alpha=17$;	$\beta=22$	

Til p adderes 1, og man faar 80; den højeste Potens af 2, som gaar op heri, er 16, som viser, at Perioden ender med 0001. 80 divideret med 16 giver 5 og $5+p=84$ er delelig med 4 (01). Kvotienten $21+p=100$ er delelig med 4 (01). Kvotienten $25+p=104$ er delelig med 8 (001). Kvotienten $13+p=92$ er delelig med 4 (01). Kvotienten $23+p=102$ er delelig med 2 (1) og saaledes videre. Tallene i den første Søjle ere alle ulige, alle forskellige og alle Rester, stemmende med at der for $2=R.$ er α ulige Rester.

Man udleder let følgende om de ulige Rester og de efterfølgende Divisorer, idet man erindrer, at p er af Formen $8n-1$:

En Rest $8n+5$ giver en Divisor 4,
— $8n+1$ — - — >4,
— $8n+3$ — - — 2, efterfulgt af en større Divisor,
— $8n+7$ — - — 2, efterfulgt af en Divisor 2.

Det er disse Rester, hvis Antal vi tidligere have betegnet henholdsvis ved ϱ_5, ϱ_1, ϱ_3 og ϱ_7, og om hvilke vi have bevist, at $\varrho_3=\varrho_5$; da nu en Rest $8n+5$ i Perioden bestemmer et isoleret Nul, medens en Rest $8n+3$ bestemmer en Rækkefølge af to eller flere 1, have vi:

I Perioden er der lige saa mange isolerede Nuller som Rækkefølger af to eller flere Ettaller,

og paa lignende Maade:

Perioden har lige saa mange isolerede Ettaller som Rækkefølger af to eller flere Nuller.

36. Hvis t er primitiv Rod, faa vi $p-1$ Cifre i Perioden; danne vi denne paa sædvanlig Maade ved Divisjon, blive Divisjonsresterne afvekslende $R.$ og $I.$ Man faar i dette Tilfælde ved Addition af Ligningerne, idet a og b henholdsvis betegne de Summer, vi faa ved at addere Periodens første, tredje, femte ... eller andet, fjerde, sjette ... Ciffer,

$$(t-1)\ (\beta+\alpha) = b + a = \text{Tværsummen},$$

og ved afvekslende at addere og subtrahere Ligningerne

$$(t+1)\ (\beta-\alpha) = b - a.$$

Saaledes have vi f. Eks. for $t = 10$

$$\frac{1}{19} = 0{,}052631578947368421\ldots;\ a = 35,\ b = 46;\ \beta-\alpha = 1.$$

Man faar det samme, naar man betragter p^2 som Grundtal, idet da de ny Cifre ere tocifrede i almindelig Forstand, og da t^2 hører til Eksponenten 9

$$(t^2-1)\,\alpha = \text{Tværsummen} = 396;\ \alpha = 4.$$

Er t primitiv Rod, blive Periodens Cifre blot kredsforskudte, naar Brøken multipliceres med et af Tallene mindre end p, da ethvert af disse Tal forekommer som Divisjonsrest. Hører t til Eksponenten $\frac{1}{2}(p-1)$, forekomme kun de kvadratiske Rester som Divisjonsrester, og kun ved Multiplikation med en af disse blive Cifrene kredsforskudte, medens man ved Multiplikation med en $I.$ faar Cifrenes Komplementer til $t-1$. Saaledes for $p = 11,\ t = 4$

$$\frac{1}{11} = 0{,}01131\ldots;\ \frac{4}{11} = 0{,}11310\ldots;\ \frac{10}{11} = 0{,}32202\ldots.$$

37. Man ser let, at dersom t er primitiv Rod, blive Periodens Cifre blot kredsforskudte, dersom vi multiplicere med et Tal, mindre end p; vi kunne derved danne Perioder uden at udføre

nogen Divisjon og uden at kende Nævneren. Lad f. Eks., idet $t=10$, de to sidste Cifre være 21 .... Tænke vi os Brøken multipliceret med 2, bliver Periodens sidste Ciffer 2, som ved Kredsforskydningen kan være kommet fra den foregaaende Plads, men da maa det foregaaende Ciffer være 4 og saaledes videre; vi finde altsaa af ethvert Ciffer det foregaaende ved Multiplikation med 2 og vedblive, til Perioden viser sig; her f. Eks. faa vi 18 Cifre, før dette sker, og den Periode, vi have dannet, er i Virkeligheden Perioden til $\frac{1}{19}$. Slutningscifrene 31 vilde ved fortsat Multiplikation med 3 give os en Periode med 28 Cifre, som i Virkeligheden er Perioden til $\frac{1}{29}$. Tage vi 51 ... faa vi en Periode med 42 Cifre; denne viser sig imidlertid ikke at være Perioden til $\frac{1}{43}$, men til $\frac{1}{49}$. I Virkeligheden er jo ogsaa

$$\varphi(49) = \varphi(43) = 42.$$

Vi have ved de nævnte Eksempler forudsat, at Multiplikationen kun forskyder Perioden eet Ciffer, og Perioden maa da tilhøre en Brøk, som ved Multiplikationen giver et Resultat, som er nær ved $\frac{1}{10}$; vi se, at dette stemmer med Eksemplerne, idet

$$\frac{2}{19}; \frac{3}{29} \text{ og } \frac{5}{49}$$

alle ere lidt større end $\frac{1}{10}$.

TREDJE KAPITEL.

I. CIRKELDELINGSLIGNINGERNE OG DERES DANNELSE.

38. Ligningen

$$x^n - 1 = 0 \tag{46}$$

har som bekendt Rødderne

$$x = \cos.\frac{2k\pi}{n} + i \sin.\frac{2k\pi}{n} \quad (k = 1, 2, 3 \ldots n-1). \tag{47}$$

Hvis $\frac{k}{n}$ kan forkortes til $\frac{k_1}{n_1}$, vil Roden ogsaa være Rod i Ligningen

$$x^{n_1} - 1 = 0,$$

saa at de Rødder i (1), der ikke tillige er Rødder i Ligninger af samme Form, men af lavere Grad, faas ved at give k de Værdier, der ere mindre end og primiske med n. Disse Rødder kaldes primitive og bestemmes ved en Ligning af Graden $\varphi(n)$, hvor φ er den bekendte talteoretiske Funktion. Ligningen af Graden $\varphi(n)$ ville vi betegne ved $\varphi_n(x) = 0$. Den kaldes en Cirkeldelingsligning, fordi den, som vist i Forfatterens „De algebraiske Ligningers Teori", tjener til Bestemmelse af den i en Cirkel indskrevne regulære n-Kants Side.

39. For at danne Cirkeldelingsligningerne kunne vi benytte følgende Sætning:

Dersom p er et Primtal, som gaar op i n, har man

$$\varphi_{np}(x) = \varphi_n(x^p), \tag{48}$$

medens, hvis p ikke gaar op i n,

$$\varphi_{np}(x) = \frac{\varphi_n(x^p)}{\varphi_n(x)}. \tag{49}$$

I det første Tilfælde have vi paa venstre Side Argumentet

$$\frac{2k\pi}{np},$$

hvor k har de Værdier, der ere mindre end np og primiske med n, som ifølge vor Forudsætning indeholder Faktoren p; paa højre Side have vi for x^p Argumentet $\frac{2k\pi}{n}$ og for x derfor Argumentet $\frac{2k\pi}{np}$, hvor k har de samme Værdier som paa venstre Side.

Den første Del af Sætningen er saaledes bevist.

I det andet Tilfælde have vi i Tælleren paa højre Side for k ogsaa de Værdier, der ere delelige med p, saa at efter Division af Argumentet med p nogle af Brøkerne kunne forkortes med p; derved faa vi Argumenterne

$$\frac{2k\pi}{n},$$

hvor k har de Værdier, der ere mindre end og primiske med n, det vil sige Argumenterne til Rødderne i $\varphi_n(x) = 0$. Af $\varphi_n(x^p)$ maa derfor Faktoren $\varphi_n(x)$ bortdivideres, naar vi skulle have den Ligning, der kun bestemmer de primitive Rødder.

40. For nu at danne $\varphi_n(x)$, danne vi først $\varphi_p(x)$, hvor p er en Primfaktor i n; dette sker ved at dividere $x^p - 1$ med $x - 1$, da 1 er den eneste af Rødderne, der ikke er primitiv; er n delelig med p^2, sætte vi nu x^p for x i det fundne Udtryk og have $\varphi_{p^2}(x)$ og saaledes videre, til vi have naaet den højeste Potens af p, der findes i n; er nu q en anden Primfaktor i n, sætte vi i det fundne Udtryk x^q for x og maa da ifølge den anden Del af Sætningen ovenfor bortdividere det φ, der svarer til den højeste Potens af p og saaledes videre.

Er f. Eks. $n = 12$, faar man

$$\varphi_2(x) = x+1;\ \varphi_4(x) = x^2+1;\ \varphi_{12}(x) = (x^6+1) : (x^2+1) = x^4 - x^2 + 1.$$

Da, hvis x er en primitiv Rod, $\frac{1}{x}$ ogsaa er det, blive Cirkeldelingsligningerne reciproke.

Er $n = 2p$, faa vi først $\varphi_2(x) = x + 1$ og derpaa

$$(50) \qquad \varphi_{2p}(x) = (x^p + 1) : (x + 1) = x^{p-1} - x^{p-2} + x^{p-3} \ldots + 1.$$

Idet vi her anføre nogle af Funktionerne $\varphi(x)$, tage vi kun saadanne, hvor n bestaar af flere forskellige Primfaktorer og ikke er det dobbelte af et Primtal.

$\varphi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$; $\varphi_{21}(x) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$; $\varphi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$;
$\varphi_{33}(x) = x^{20} - x^{19} + x^{17} - x^{16} + x^{14} - x^{13} + x^{11} - x^{10} + x^9 \ldots - x + 1$;
$\varphi_{35}(x) = x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} + x^{12} \ldots$;
$\varphi_{39}(x) = x^{24} - x^{23} + x^{21} - x^{20} + x^{18} - x^{17} + x^{15} - x^{14} + x^{12} \ldots\ldots + 1$.

Koefficienterne ere alle 1, 0 og -1, men dette udtrykker ikke nogen almindelig Sætning, men gælder kun, til man naar $n = 105$.

41. Man har straks $\varphi_p(1) = p$, og ifølge Ligningernes Dannelsesmaade maa det samme gælde, hvis Indeks er en højere Potens af Primtallet p. Hvis man tilføjer en ny Primfaktor, faar i (49) Tæller og Nævner samme Værdi for $x = 1$. Man har saaledes, naar Indeks er en Potens af et Primtal,

$$\varphi_{p^\alpha}(1) = p \tag{51}$$

og i alle andre Tilfælde

$$\varphi_n(1) = 1. \tag{52}$$

42. Koefficienten til andet Led i $\varphi_n(x)$ er $-\mu(n)$.

Tallet $\mu(n)$ betyder som bekendt 0, naar n er deleligt med et Kvadrattal, $+1$, naar n bestaar af et lige Antal forskellige Primfaktorer, -1, hvis Antallet er ulige. Man ser nu straks, at Sætningen er rigtig, naar n er et Primtal; er n delelig med p^n, hvor p er et Primtal, kan man tilføje Faktoren p sidst, og da dette sker ved at rette x til x^p, bliver Koefficienten til andet Led Nul; ere alle Primfaktorerne i n forskellige, bliver i (48) den anden Koefficient i Tælleren Nul og derfor i Brøken, naar Divisjonen er udført, den samme som i Nævneren, men med modsat Fortegn; da nu Koefficienten er $+1$, for een Primfaktor, bliver den -1 for to og saaledes videre.

Vi kunne nu let bestemme Røddernes Potenssummer; er s_r Summen af Røddernes r^{te} Potenser, og er r primisk med n,

bliver i (47) Værdierne af kr kongruente med Værdierne af k for Mod. n, og vi faa derfor $s_r = s_1$. Er $r = fr_1$, hvor f er største fælles Maal for n og r, kunne vi først opløfte Rødderne til Potensen r_1, hvorved blot deres Orden forandres; idet vi nu opløfte til Potensen f, dividere vi Argumenternes Nævner med f, og faa derved Rødderne i

$$\varphi_{n:f}(x) = 0,$$

men hver af dem f Gange. Vi have altsaa:

Summen af de r^{te} Potenser af Rødderne i $\varphi_n(x) = 0$ er f Gange Summen af Rødderne i $\varphi_{n:f}(x) = 0$, hvor f betyder st. f. M. for n og r.

43. Idet 1, d_1, d_2 ... ere Divisorerne i n, er

$$\varphi_n(x) \cdot \varphi_{d_1}(x) \cdot \varphi_{d_2}(x) \ldots (x-1) = x^n - 1. \tag{53}$$

Ifølge en bekendt Sætning i Talteorien er

$$\varphi(n) + \varphi(d_1) + \varphi(d_2) + \ldots = n,$$

saa at Produktet paa venstre Side af (53) er af n^{te} Grad, og de Rødder, det bestemmer, naar vi sætte det lig Nul, ere alle Rødder i Ligningen $x^n = 1$; de ere tillige alle forskellige, da en Størrelse ikke kan være primitiv Rod i to forskellige Ligninger.

44. Vi saa ovenfor, at hvis α er Rod i Ligningen $\varphi_n(x) = 0$, da er α^r det ogsaa, hvis r er primisk med n; da der nu er $\varphi(n)$ Tal, der ere mindre end og primiske med n, faar man, ved at benytte alle disse Værdier, alle Ligningens Rødder bragte paa Formen α^r. Er $n = p$ (Primtal), faa vi saaledes alle Rødderne skrevne som

$$\alpha, \alpha^2, \alpha^3, \ldots \alpha^{p-1},$$

hvor α er en hvilken som helst af Rødderne. Er i Almindelighed r primisk med n, kunne Rødderne ogsaa skrives

$$\alpha, \alpha^r, \alpha^{r^2}, \alpha^{r^3} \ldots,$$

men i denne Række faa vi kun alle Rødderne med, hvis r er en primitiv Rod for Kongruensen

$$x^{\varphi(n)} - 1 \equiv 0 \pmod{n}.$$

Naar vi tale om at opløfte alle en Lignings Rødder til en vis Potens, ville vi derved forstaa, at vi tænke os den Ligning dannet, hvis Rødder ere den nævnte Potens af den givne Lignings Rødder. Opløfte vi Rødderne i $\varphi_n(x)$ til r^{te} Potens, hvor r er primisk med n, faa vi de samme Rødder, blot i en anden Orden, og Ligningen bliver derfor uforandret.

II. CIRKELDELINGSLIGNINGERNES IRREDUKTIBILITET.

45. Naar vi, ved at bortfjerne Faktorer af $x^n - 1$, ere komne til Polynomiet $\varphi_n(x)$, opstaar det Spørgsmaal, om dette Polynomium atter kan deles i rationale Faktorer, eller om det er irreduktibelt. Dette sidste er i Virkeligheden Tilfældet, men det varede længe, før det lykkedes at føre Bevis herfor. Gauss kom stadig tilbage til Opgaven, men naaede kun at føre Beviset for det Tilfælde, hvor n er et Primtal. Andre Beviser, tildels ogsaa for det Tilfælde, hvor n er en Potens af et Primtal, gaves af Kronecker*), Schönemann, Eisenstein o. fl., medens endelig den almindelige Sætning bevistes af Dedekind**) og Arndt***).

46. Førend vi gaa over til at give et Par ny, meget simple Beviser, ville vi føre et nyt Bevis for en Sætning, som vi faa Brug for.

Lad

$$(54) f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} \ldots + a_n = (x - x_1)(x - x_2) \ldots (x - x_n) = 0$$

være en algebraisk Ligning af n^{te} Grad med hele Koefficienter og med Rødderne $x_1, x_2 \ldots, x_n$. Vi opløfte paa begge Sider

---

*) Crelles Journal, Bd. 29.
**) — — — 54.
***) — — — 56.

til p^{de} Potens, hvor p er et ulige Primtal. Paa venstre Side faa vi

$$x^{np} + a_1^p x^{(n-1)p} + a_2^p x^{(n-2)p} + \ldots + p A,$$

hvor A er et Polynomium med hele Koefficienter, hvis Leds Eksponenter kunne være eller ikke være delelige med p. Paa den anden Side af Lighedstegnet sætte vi

$$(x - x_k)^p = x^p - x_k^p - p\,(x^{p-1} x_k - \frac{p-1}{2} x^{p-2} x_k^2 + \ldots),$$

saa at Produktet bliver

$$(x^p - x_1^p)(x^p - x_2^p) \ldots (x^p - x_n^p) + p B, \tag{55}$$

hvor B er et Polynomium, hvis Koefficienter ere symmetriske Funktioner af Rødderne og derfor kunne udtrykkes uden Brøk ved a_1, $a_2 \ldots a_n$. Det samme gælder om det første Led, hvor vi dog kun faa saadanne Eksponenter for x, som ere delelige med p. Vi have saaledes faaet to identiske Udtryk, og vi maa atter faa en Identitet, hvis vi begge Steder kun benytte de Led, hvis Eksponenter ere delelige med p, og heri overalt sætte x for x^p; vi faa derved

$$x^n + a_1^p x^{n-1} + a_2^p x^{n-2} \ldots + a_n^p \equiv (x - x_1^p)(x - x_2^p) \ldots (x - x_n^p) \pmod{p}. \tag{56}$$

Da nu ifølge Fermats Sætning

$$a^p \equiv a \pmod{p},$$

have vi Sætningen:

Dersom vi af en Ligning, hvis Koefficienter ere hele Tal, den første lig 1, danne den Ligning, hvis Rødder ere de p^{de} Potenser af den førstes, da ere de to Ligningers Koefficienter parvis kongruente for Modolus p. (p Primtal).

47. Vi vende os nu til vort Bevis for Irreduktibiliteten af $\varphi(x)$ og bevise her først følgende Sætning:

Dersom Ligningen $\varphi(x) = 0$ er reduktibel, maa de irreduktible Ligninger, i hvilke den deler sig, være af samme Grad.

Lad to af disse Ligninger være

$$\psi_1(x) = 0 \text{ og } \psi_2(x) = 0,$$

og α være en Rod i den første, medens α^k er en Rod i den anden. Alle Polynomierne ψ have ifølge 39 hele Koefficienter, den første lig 1. Dersom man opløfter alle Rødderne i den første Ligning til Potensen k, faar man en Ligning, der har en Rod fælles med den anden Ligning, og den maa da, da denne er irreduktibel, have dem alle; den første Ligning kan da ikke være af lavere Grad end den anden.

Paa samme Maade ser man, at den anden Ligning ikke kan være af lavere Grad end den første, og vor Sætning er saaledes bevist.

48. Vi ville nu, nærmest af historiske Grunde, føre Beviset for Irreduktibiliteten for $n = p^a$, uagtet Beviset for det almindelige Tilfælde næsten er lige saa simpelt.

Ifølge 41 maa en af Funktionerne ψ f. Eks. ψ_1 for $x = 1$ have Værdien $\pm p$, medens alle de andre faa Værdien ± 1; vi have da, uden Hensyn til Fortegnet,

$$\frac{1}{p} = \frac{\psi_2(1)}{\psi_1(1)} = \frac{(1-\alpha_1^k)(1-\alpha_2^k)\ldots}{(1-\alpha_1)(1-\alpha_2)\ldots},$$

hvor $\alpha_1, \alpha_2 \ldots$ ere Rødderne i $\psi_1(x) = 0$. Udføres Divisjonen, faa vi en symmetrisk Funktion af Rødderne i $\psi_1(x) = 0$ med hele Tal til Koefficienter; Sætningen er derved bevist, da Værdien af en saadan Funktion er et helt Tal og derfor ikke kan være $\frac{1}{p}$.

49. Vi ville nu gaa over til Beviset for den almindelige Sætning.

Antag

$$\varphi_n(x) = \psi_1(x)\,\psi_2(x)\ldots,$$

hvor Rødderne i $\psi_2(x) = o$ ere de k^{de} Potenser af Rødderne i $\psi_1(x) = 0$, og k er primisk med n. Lad $m > n$ være et Tal, der er større end ethvert Tal, der gaar op i alle Koefficienterne i alle Udtrykkene

$$\psi_i(x) - \psi_j(x)$$

og

$$t = An + k,$$

hvor A betyder Produktet af alle Primtal op til m med Undtagelse af de Primfaktorer, der findes i k. Opløfte vi alle Rødderne i $\psi_1(x) = 0$ til Potensen t, faa vi, da $x^n = 1$, Ligningen $\psi_2(x) = 0$.

Antag

$$t = P_1 P_2 P_3 \ldots,$$

hvor Tallene P ere Primtal, der ifølge vor Forudsætning om Tallet A alle maa være større end m. Opløfte vi nu alle Rødderne i $\psi_1(x) = 0$ til Potensen P_1, derpaa disse Rødder til Potensen P_2 og saaledes videre, kunne vi ikke stadig komme til Ligningen $\psi_1(x) = 0$, da vi maa ende med $\psi_2(x) = 0$. Der maa derfor være en af Potensopløftningerne, f. Eks. den til Potensen P_3, der fører os fra $\psi_1(x)$ f. Eks. til $\psi_i(x)$; i dette Tilfælde maa ifølge 46 P_3 gaa op i alle Koefficienterne i

$$\psi_1(x) - \psi_i(x),$$

men da $P > m$ strider dette mod vor Forudsætning om Tallet m.

Alle Ligninger $\varphi_n(x) = 0$ ere saaledes beviste at være irreduktible.

III. DISKREMINANTEN TIL $\varphi_n(x) = 0$.

50. Vi ville betegne Diskreminanten til $\varphi_n(x) = 0$ ved D_n; vi have da, som bekendt fra Ligningernes Teori (uden Hensyn til Fortegnet),

$$D_n = \varphi'_n(x_1)\,\varphi'_n(x_2)\ldots,$$

idet $x_1, x_2, \ldots$ ere alle Ligningens Rødder. Er nu $n = p$, have vi

$$\varphi_p(x) = \frac{x^p - 1}{x - 1},$$

hvoraf

$$\varphi'_p(x) = \frac{px^{p-1}}{x-1} - \frac{x^p-1}{(x-1)^2},$$

hvor det sidste Led bliver Nul for $x = x_1, x_2 \ldots$, saa at

$$\varphi'_p(x_\alpha) = \frac{px_\alpha^{p-1}}{x_\alpha - 1},$$

Da nu Produktet af alle Rødderne er 1 og

$$(1-x_1)(1-x_2)\ldots = p,$$

faar man (numerisk)

$$D_p = p^{p-2}. \tag{57}$$

51. Antage vi nu $n = \alpha p$, hvor α er delelig med p, har man

$$\varphi_{\alpha p}(x) = \varphi_\alpha(x^p),$$

hvoraf

$$\varphi'_{\alpha p}(x) = px^{p-1}\varphi'_\alpha(x^p).$$

Da man ved at opløfte alle Rødderne i $\varphi_{\alpha p}(x)=0$ til p^{de} Potens faar alle Rødderne i $\varphi_\alpha(x) = 0$, hver p Gange, følger heraf

$$D_{\alpha p} = p^{\varphi(\alpha p)} D_\alpha^p \ (\alpha \text{ delelig med } p). \tag{58}$$

Er α ikke delelig med p, har man ifølge (49)

$$\varphi_{\alpha p}(x) = \varphi_\alpha(x^p) : \varphi_\alpha(x),$$

hvoraf, idet vi bortkaste det Led, der blive Nul for alle Rødderne,

$$\varphi'_{\alpha p}(x) = px^{p-1}\varphi'_\alpha(x^p) : \varphi_\alpha(x),$$

altsaa:

$$D_{\alpha p} = p^{\varphi(\alpha p)} D_\alpha^{p-1} : \Pi\varphi_\alpha(x_i), \tag{59}$$

hvor x_i har $(p-1)\varphi(\alpha)$ Værdier.

52. Lad nu $\alpha_1, \alpha_2, \alpha_3 \ldots$ være de $\varphi(\alpha)$ Rødder i $\varphi_\alpha(x) = 0$; vi have da, uden Hensyn til Fortegnet,

$$\varphi_\alpha(x) = (\alpha_1 - x)(\alpha_2 - x)\ldots,$$

altsaa for $x = x_i$

$$\varphi_\alpha(x_i)=(\alpha_1-x_i)(\alpha_2-x_i)\ldots=\alpha_1\alpha_2\ldots(1-\alpha_1^{-1}x_i)(1-\alpha_2^{-1}x_i)\ldots$$

eller, da Produktet af Rødderne α er 1 og a_j^{-1} er en fra α_j forskellig Rod

$$\Pi\varphi_\alpha(x_i) = \Pi(1-\alpha_j x_i),$$

der viser, at det søgte Produkt findes, naar vi sætte $x = 1$ i venstre Side af den Ligning, hvis Rødder ere alle Produkter $\alpha_j x_i$. Disse Rødder tilfredsstille alle Ligningen

$$x^{\alpha p} = 1. \tag{60}$$

Er x_1 en af Rødderne x, kunne de alle skrives som x_1^β, hvor β betyder alle Tal mindre end og primiske med $p\alpha$. x_1^p er en af Rødderne α, og alle disse fremstilles derfor ved $x^{\gamma p}$, hvor γ betegner Tallene mindre end og primiske med α; den Ligning, vi skulle danne, faar derfor Rødderne

$$x_1^{\gamma p+\beta}$$

og faar rationale Koefficienter, da vi for x_1 kunne sætte enhver anden af Rødderne x; den maa være sammensat af en eller flere af de irreduktible Ligninger, i hvilke (60) deler sig.

Nu have vi imidlertid ifølge (51) og (52), at $\varphi_n(1)$ i alle er 1, undtagen naar n er en Potens af et Primtal. Spørgsmaalet bliver derfor, i hvilke Tilfælde i Røddernes Argumenter

$$2\pi\frac{\gamma p+\beta}{\alpha p}$$

Brøken kan forkortes, saa at Nævneren bliver Potens af et Primtal; da p ikke gaar op i Tælleren, kan dette Primtal kun være p, og da α ikke er delelig med p, have vi saaledes kun at undersøge, naar α gaar op i Tælleren eller, naar

$$p\gamma+\beta\equiv 0. \pmod{\alpha}.$$

Da nu α er primisk med p, har denne Kongruens netop een Løsning for hver Værdi af β, og der er saaledes $\beta=(p-1)\varphi(\alpha)$ Rødder, der tilfredsstille Ligningen

$$\varphi_p(x) = 0,$$

og da denne har $p-1$ Rødder, maa den forekomme $\varphi(\alpha)$ Gange; for hver Gang har man $\varphi_p(1) = p$, og vi have saaledes fundet

$$\Pi\varphi_\alpha(x_i) = p^{\varphi(\alpha)},$$

som, indsat i Udtrykket for Diskriminanten, giver

$$D_{\alpha p} = p^{\left(1-\frac{1}{p-1}\right)\varphi(\alpha p)} D_\alpha^{p-1} \quad (\alpha \text{ pr. med } p). \tag{61}$$

51. Vi kunne nu ved successiv Benyttelse af de fundne Formler finde Diskreminanten for alle Tilfælde; er n opløst i Primfaktorer

$$n = p^\alpha q^\beta r^\gamma \ldots,$$

faa vi

$$D_n = \left(p^{\alpha-\frac{1}{p-1}} q^{\beta-\frac{1}{q-1}} r^{\gamma-\frac{1}{r-1}} \ldots \right)^{\varphi(n)}. \tag{62}$$

Vi se heraf, at:

Diskreminanten til Ligningen $\varphi_n(x) = 0$ har de samme Primfaktorer som n og ingen andre.

52. Cirkeldelingsligningerne høre til de Abel'ske Ligninger, hvis Rødder danne een Gruppe; om disse vises det i de algebraiske Ligningers Teori, at de kunne løses ved Roduddragninger, og at den første Rod, der bliver at uddrage, er Kvadratroden af Diskreminanten (positiv eller negativ); vi ville derfor undersøge, i hvilke Tilfælde dennes numeriske Værdi er et Kvadrattal*). Nu er

$$\varphi(n) = p^{\alpha-1} \cdot q^{\beta-1} \ldots (p-1)(q-1)\ldots,$$

og indsættes dette Udtryk i (62), faa vi en Eksponent for p, der indeholder de lige Faktorer $q-1$, $r-1\ldots$; vi se altsaa, at Diskreminanten altid er et Kvadrattal, naar n har flere end

---

*) Man plejer at give Diskreminanten til en Ligning af n^{te} Grad Fortegnet $(-1)^{\frac{1}{2}n(n-1)}$.

1 ulige Primfaktor, medens Eksponenten bliver ulige, naar n er en Potens af et ulige Primtal eller det dobbelte af en saadan Potens. Vi faa altsaa (bortset fra Tallene 2 og 4):

Diskreminanten til en Cirkeldelingsligning $\varphi_n(x) = 0$ er altid et Kvadrattal, hvis n ikke er et af de Tal, der har primitive Rødder, i hvilke Tilfælde den ulige Primfaktor faar ulige Eksponent, saa at Ligningens Løsning kræver en Kvadratrodsuddragning af dette Tal.

IV. DIVISORERNE I $\varphi_n(x)$.

53. Antag, at p er et Primtal, som gaar op i $x^n - 1$ for en vis Værdi af x, og som ogsaa gaar op i n, saa at $n = mp$. Vi have da

$$(63) \quad x^n - 1 = (x^m - 1)(x^{m(p-1)} + x^{m(p-2)} + \ldots + x^m + 1).$$

Her giver ethvert af Leddene i den sidste Parentes, divideret med $x^m - 1$ Resten 1 og hele Parentesen altsaa Resten p. Heraf følger:

De to Faktorer i Parenteserne maa for enhver Værdi af x enten være indbyrdes primiske eller have p til største fælles Maal.

Da $x^p \equiv x \pmod{p}$, bliver $x^{mp} \equiv x^m$; er m delelig med p, slutte vi videre paa samme Maade, til vi komme til en Eksponent, der ikke er delelig med p. Vi bevise nu paa samme Maade som ved en analog Sætning i Talteorien, at hvis p^α er den højeste Potens af p, der gaar op i $x^m - 1$, saa er $p^{\alpha+1}$ den højeste Potens, der gaar op i $x^{mp} - 1$ og have saaledes, idet $n = kp^\beta$, hvor k ikke er delelig med p:

Hvis den højeste Potens af p, der gaar op i $x^k - 1$, er p^μ, saa er $p^{\mu+\beta-1}$ den højeste Potens, der gaar op i $x^m - 1$ og p den højeste Potens, der gaar op i den anden Faktor.

54. Vi beviste i 43, at

$$(64) \qquad x^n - 1 = \Pi \varphi_d(x); \; x^m - 1 = \Pi \varphi_{d_1}(x),$$

hvor Mærkerne henholdsvis svare til alle Divisorer i n og m. Den anden Faktor i (63) maa derfor være Produktet af alle de φ, hvis Mærketal ere Divisorer i n, men ikke i m, det vil sige de Divisorer, som indeholde Faktoren p^β, altsaa:

Af alle de φ, hvis Mærketal ere delelige med den højeste Potens af p, der gaar op i n, er et og kun eet delelig med p og det kun med p i første Potens for enhver Værdi af x. Iblandt disse er $\varphi_n(x)$.

55. Vi ville nu undersøge, hvilken af Faktorerne det er, der for en given Værdi af x, er delelig med p.

Lad x høre til Eksponenten α for Mod. p. Da p gaar op i $x^k - 1$, hvor k ikke er delelig med p, og i $x^{p-1} - 1$ (idet x er primisk med p), er α fælles Faktor for k og $p - 1$. Er nu $k = t\alpha$ og $x^\alpha = 1 + ap^s$, hvor a ikke er delelig med p, bliver

$$(65) \; x^k - 1 = (1 + ap^s)^t - 1 = atp^s + \text{Led med højere Eksponenter for } p.$$

Den højeste Potens af p, der gaar op i $x^k - 1$ og i $x^\alpha - 1$, er derfor den samme, og det samme gælder da om

$$x^{kp^\beta} - 1 \text{ og } x^{\alpha p^\beta} - 1,$$

saa at disses Forhold ikke er deleligt med p. Men dette Forhold indeholder $\varphi_n(x)$ som Faktor, og $\varphi_n(x)$ er saaledes ikke delelig med p. Herfra undtages dog Tilfældet $\alpha = k$. Vi have herved naaet vort første Resultat:

Er p en Primfaktor i n og $n = kp^\beta$, hvor k ikke er delelig med p, kan p gaa op i $\varphi_n(x)$, men kun i første Potens, og dette finder Sted for saadanne Værdier af x, der høre til Eksponenten k for Mod. p.

Lad nu q være et Primtal, der gaar op i $x^n - 1$ for en vis Værdi af x, men ikke gaar op i n, og lad x høre til Eks-

ponenten α for Mod. q. α maa da gaa op i n, saa at f. Eks. $n = k\alpha$; lad q^β være den højeste Potens af q, der gaar op i $x^\alpha - 1$, saa at

$$x^\alpha = aq^\beta + 1$$

og

(66) $x^n - 1 = (aq^\beta + 1)^k = kaq^\beta +$ Led med højere Eksponenter for q,

der, da hverken a eller k ere delelige med q, viser, at $x^\alpha - 1$ og $x^n - 1$ ere delelige med samme Potens af q, saa at deres Forhold ikke er deleligt med q. For $\alpha < n$ indeholder dette Forhold imidlertid Faktoren $\varphi_n(x)$. Skal q gaa op i $\varphi_n(x)$, maa α derfor høre til Eksponenten n for Mod. q. Dette kræver, at n gaar op i $q - 1$, saa at vi have:

En Primfaktor, der gaar op i $\varphi_n(x)$ for en vis Værdi af x og ikke gaar op i n, maa have Formen

$$an + 1,$$

og x maa for Primfaktoren som Modulus høre til Eksponenten n.

Heraf følger, at de irreduktible Faktorer i $x^n - 1$ for samme Værdi af x ikke kunne have nogen Primfaktor $an + 1$ fælles; hvis nemlig Primtallet $an+1$ gik op baade i $\varphi_{d_1}(\alpha)$ og i $\varphi_{d_2}(\alpha)$, maatte α baade høre til Eksponenten d_1 og til Eksponenten d_2 for samme Primtalsmodulus, hvilket er umuligt. Om en Primfaktor i n have vi set, at den kan findes i flere af Faktorerne φ. Saaledes for $n = 18$, $x = 4$ gaar 3 op i φ_2, φ_3 og φ_9.

56. *Lejeune Dirichlet* har bevist den Sætning, at der i en uendelig Differensrække, hvor første Led og Differensen ere indbyrdes primiske, findes uendelig mange Led, der ere Primtal. Hans Bevis for denne Sætning er meget sammensat og kræver Hjælpemidler, der gaa langt ud over den elementære Aritmetik. For det specielle Tilfælde, hvor første Led er 1, kunne vi nu imidlertid føre et meget simpelt Bevis.

Lad n være Differensen og antag, at der kun findes et endeligt Antal Primtal af Formen $an + 1$. Lad P være Produktet af disse Primtal og lad os i $\varphi_n(x)$ sætte $x = nP$; det Tal, vi derved faa, kan hverken være deleligt med en Faktor i n eller i P; da nu ifølge Sætningen ovenfor alle dets Primfaktorer have Formen $an + 1$, maa der være flere saadanne end dem, der findes i P. Altsaa:

I en uendelig Differensrække, hvis første Led er 1, findes uendelig mange Primtal.

57. Lad os nu antage, at der i Primtalrækken kun blev et endeligt Antal tilbage, naar alle af Formen $an + 1$ borttoges; lad P nu betyde Produktet af de tilbageblevne, og lad os betragte Tallet

$$nP - 1.$$

I dette kan ikke noget af de tilbageblevne gaa op, og det maa derfor være sammensat af Primfaktorer af Formen $an + 1$. Produktet af Tal af denne Form faar imidlertid samme Form og kan derfor ikke være $Pn - 1$.

Da nu alle ulige Primtal har en af Formerne $4a + 1$ og $4a - 1$ og en af Formerne $6a + 1$ og $6a - 1$ følger heraf:

Der er uendelig mange Primtal af Formen $4a - 1$ og ligeledes af Formen $6a - 1$.

Hvor der er flere end to mulige første Led, kan man kun af det beviste slutte, at for mindst et af dem foruden 1 er Primtalmængden uendelig.

58. Dersom vi i Stedet for $x^n - 1$ sætte $x^n - y^n$, hvor x og y skulle tænkes indbyrdes primiske, vedbliver hele vor Udvikling at gælde, idet blot vore Ligninger blive homogene i x og y. Vi sætte

$$\varphi_n(x, y) = y^{\varphi(n)}\, \varphi\left(\frac{x}{y}\right)$$

og sige, at Tallene x og y ere primitive Rødder i Ligningen $x^n - y^n = 0$, naar de tilfredsstille denne Ligning, men ikke nogen anden Ligning af samme Form, men af lavere Grad; det er i Virkeligheden kun deres Forhold, det kommer an paa, og det er dette, der skal være primitiv Rod i Ligningen $x^n - 1 = 0$. Er $\varphi_n(x)$ opløst i sine irreduktible Faktorer, og gøre vi disse homogene ved Multiplikation af Leddene med passende Potenser af y, faa vi $\varphi_n(x, y)$ opløst i Faktorer, og af denne Opløsning faa vi atter den første ved at sætte $y = 1$.

Vi have saaledes den almindelige Sætning:

Naar x og y ere hvilke som helst indbyrdes primiske Tal, kan $\varphi_n(x, y)$ ikke indeholde andre Primfaktorer end saadanne, som findes i n og saadanne, som ere af Formen $an + 1$, de første kun i første Potens.

Af denne Sætning have vi tidligere omtalt Tilfældene $n = 4$, hvor man har

$$\varphi_4(x, y) = x^2 + y^2 \tag{67}$$

med Divisorerne 2 og Primtal af Formen $4a + 1$. For $n = 6$ faar man

$$\varphi_6(x, y) = x^2 - xy + y^2 \tag{68}$$

med Divisorerne 3 og Primtal af Formen $6a + 1$.

V. KONGRUENSEN $\varphi_n(x) \equiv 0$.

59. Idet vi have fundet Formen af de Primtal, der kunne gaa op i $\varphi_n(x)$ for alle Værdier af x, have vi tillige bestemt de Primtalsmoduler, for hvilke Kongruensen

$$\varphi_n(x) \equiv 0 \pmod{p} \tag{69}$$

kan have Løsninger. Idet vi se bort fra Divisorerne i n ere disse Primtal

$$p = an + 1,$$

hvor vi imidlertid have tilbage at undersøge, om der ogsaa gives Løsninger for alle saadanne Primtal; nu have vi imidlertid for et vilkaarligt Primtal $an+1$, at n er Divisor i $p-1$, og vi have bevist, at p gaar op i $\varphi_n(x)$ for de Værdier af x, der for Mod. p høre til Eksponenten n. Af disse gives der ifølge en bekendt Sætning i Talteorien $\varphi(n)$, som netop er det Antal Rødder Kongruensen maa have. Altsaa:

Kongruensen

$$\varphi_n(x) \equiv 0 \pmod{p = an + 1}$$

har $\varphi(n)$ Rødder, som netop ere de $\varphi(n)$ Tal, der for Mod. p høre til Eksponenten n.

Da Kongruensen netop har saa mange Rødder, som dens Grad angiver, kunne vi ved disse opløse $\varphi_n(x)$ i $\varphi(n)$ lineære Faktorer og ved Udførelse af Multiplikationen og Sammenligning af Koefficienterne faa Røddernes symmetriske Summer bestemte. Man maa imidlertid erindre, at denne Bestemmelse gælder for Mod. p, og at der til det samme n svarer uendelig mange p.

Lad os f. Eks. betragte Røddernes Sum; om den have vi:

Summen af Rødderne i Kongruensen $\varphi_n(x) = 0$ er kongruent med $\mu(n)$, og dette gælder for enhver Modulus, der er et Primtal af Formen $an + 1$.

Lad os f. Eks. tage $\varphi_6(x) = x^2 - x + 1$. Sætte vi $p = 7$, faa vi Rødderne 3 og $3^5 \equiv 5$, Summen altsaa $8 \equiv 1 = \mu(6)$. For $p = 13$ ere Rødderne 4 og 10, for $p = 31$ ere de 6 og 26 o. s. v.

FJERDE KAPITEL.

I. OM $\varphi_p(x)$, HVOR PRIMTALLET p ER AF FORMEN $4n+3$.

60. Idet vi sætte

$$\varrho = \cos.\frac{2\pi}{p} + i \sin.\frac{2\pi}{p}, \tag{70}$$

kunne alle Rødderne i Ligningen $\varphi_p(x) = 0$ skrives som

$$\varrho, \varrho^2, \varrho^3 \ldots \varrho^{p-1}.$$

Disse Rødder kunne deles i to Grupper med $\frac{1}{2}(p-1)$ i hver, idet den ene bestaar af dem, hvor Eksponenterne ere *R.*, den anden af dem, hvor Eksponenterne ere *I.* for p. Lad y_1 og y_2 henholdsvis betegne Summen af Rødderne i den første og i den anden Gruppe, man har da

$$y_1 + y_2 = -1. \tag{71}$$

Udtrykket

$$y_1 - y_2$$

har to Værdier, thi indsætte vi for ϱ en anden af Rødderne ϱ^n, vil y_1 og y_2 blive uforandrede, hvis n er en *R.*, men ombyttes, hvis n er en *I.* Vi ville beregne Produktet $y_1 y_2$, der kun har een Værdi og derfor maa være rationalt.

Ved Multiplikationen faa vi $\frac{1}{4}(p-1)^2$ Led; af disse ere $\frac{1}{2}(p-1)$ lig 1, da der til et Led ϱ^r i den ene Sum svarer et Led ϱ^{p-r} i den anden Sum. Tilbage er der en Sum af $\frac{1}{4}(p-3)(p-1)$ Led, der alle ere komplekse Rødder i $\varphi_p(x)=0$, og da denne Ligning er irreduktibel, maa i Summen, hvis Værdi er rational, enhver af dens Rødder forekomme lige mange Gange, nemlig $\frac{1}{4}(p-3)$ Gange; vi finde saaledes

$$y_1 y_2 = \frac{1}{2}(p-1) + \frac{1}{4}(p-3)(-1) = \frac{1}{4}(p+1), \tag{72}$$

saa at y_1 og y_2 ere Rødderne i Ligningen

$$y^2 + y + \frac{1}{4}(p+1) = 0,$$

hvoraf

$$\left.\begin{matrix} y_1 \\ y_2 \end{matrix}\right\} = \frac{-1 \pm \sqrt{-p}}{2}. \tag{73}$$

Dette stemmer med den fra Ligningernes Teori bekendte Sætning, at en Funktion af Rødderne, der har to Værdier (en alternerende Funktion), kan udtrykkes rationalt ved Kvadratroden af Ligningens Diskreminant, idet denne her, naar vi tage Hensyn til Fortegnet, er $-p^{p-2}$ (57).

Det var let nok at finde den kvadratiske Ligning, men den Opgave at bestemme, hvilket Fortegn, der skal benyttes for y_1, har vist sig særdeles vanskelig, og det var først efter lange Tiders forgæves Forsøg, at det lykkedes *Gauss* at bevise, at:

Med den angivne Betydning af ϱ, skal man for y_1 bruge Fortegnet + eller med andre Ord, man har

$$y_1 - y_2 = +\sqrt{-p}. \tag{74}$$

61. Vi ville nu betragte de to Ligninger af Graden $\frac{1}{2}(p-1)$, hvis Rødder ere henholdsvis den første og den anden Gruppe. Med den sædvanlige Betegnelse for Røddernes Potenssummer have vi henholdsvis

$$s_1 = y_1 \text{ og } s_1 = y_2,$$

og da vi ved at opløfte Rødderne i den første Gruppe til n^{te} Potens faa Rødderne i den samme eller i den anden Gruppe, eftersom n er en *R.* eller en *I.*, faa Potenssummerne kun Værdierne y_1 og y_2, nemlig for den første Ligning

$$s_r = y_1;\ s_i = y_2, \tag{75}$$

og omvendt for den anden Ligning. Af Potenssummerne kan man nu ved Hjælp af Newtons Formler beregne Koefficienterne, men da denne Beregning ikke giver nogen Forstaaelse af disses almindelige Karakter, ville vi gaa en anden Vej.

62. De to Ligninger, der begge ere af Graden $\frac{1}{2}(p-1)$, ere irreduktible, selv om $\sqrt{-1}$ tages som en tilføjet Størrelse, thi hvis de vare reduktible, vilde deraf straks følge Reduktibiliteten af $\varphi_p(x) = 0$. Vi behøve kun at betragte den første Ligning, da den anden udledes af den, naar man overalt forandrer Fortegnet for $\sqrt{-p}$.

Koefficienten til $x^{\frac{1}{2}(p-1)-q}$ er $(-1)^q$, multipliceret med Summen af Produkterne af q og q af Rødderne; af disse Produkter er der $K_{\frac{1}{2}(p-1),q}$, og de ere alle Rødder i $x^p - 1 = 0$. Lad c_q af dem være 1; paa Grund af de to Ligningers Irreduktibilitet, maa de, der hører til y_1, forekomme lige mange Gange og ligeledes de, der høre til y_2. Idet disse Antal Gange henholdsvis betegnes ved a_q og b_q, faar Koefficienten Formen

$$(-1)^q(a_q y_1 + b_q y_2 + c_q),$$

hvor

$$\frac{1}{2}(p-1)(a_q + b_q) + c_q = K_{\frac{1}{2}(p-),q} = K_q. \tag{76}$$

Kalde vi Koefficienten A_q, og indføre vi Værdierne af y_1 og y_2, faa vi saaledes

$$A_q = (-1)^q\left(-\frac{1}{2}(a_q + b_q) + c_q + \frac{1}{2}(a_q - b_q)\sqrt{-p}\right), \tag{77}$$

hvor der ikke forekommer andre Nævnere end 2, saa at vi, naar vi multiplicere Ligningernes venstre Side med 2, faa lutter hele Koefficienter. Vi kunne da skrive Ligningen som

$$0 = Y - \sqrt{-p}\,Z = 2x^{\frac{1}{2}(p-1)} + x^{\frac{1}{2}(p-3)} + \ldots - \sqrt{-p}\,(x^{\frac{p-3}{2}} + \ldots). \tag{78}$$

Ved her at ombytte Fortegnet for $\sqrt{-p}$, faar man den Ligning, der bestemmer Rødderne ϱ^i og derpaa ved Multiplikation Identiteten

$$Y^2 + pZ^2 = 4(x^{p-1} + x^{p-2} + \ldots + x + 1). \tag{79}$$

Hvis man i (78) ombytter Rødderne med deres reciproke Værdier, maa, da -1 er *I.*, Ligningen gaa over til

$$\pm(Y + \sqrt{-p}\,Z) = 0.$$

Her maa nederste Fortegn benyttes, thi Røddernes Produkt er 1 og, da Ligningen er af ulige Grad, sidste Led negativt. Y gaar altsaa over til $-Y$, medens Z bliver uforandret, altsaa:

Koefficienterne i Y ere symmetriske med modsatte, medens de i Z ere symmetriske med samme Tegn.

Heraf følger, at Y bliver Nul for $x = 1$, medens Z bliver Nul for $x = 0$ og for $x = -1$, altsaa:

Y er delelig med $x - 1$, medens Z er delelig med $x(x + 1)$.

Ved i Identiteten (79) at sætte $x = +1$ og $x = -1$ finder man, at Z^2 i det første Tilfælde og Y^2 i det andet Tilfælde faa Værdien 4, altsaa Z og Y Værdierne ± 2; den nærmere Bestemmelse af Fortegnet vil senere blive omtalt.

63. Vi vende nu tilbage til Koefficienterne. I den reelle Del af disse kunne vi ved (76) bortskaffe c_q eller $a_q + b_q$ og faa derved for Koefficienterne i Y henholdsvis

$$A_q = (-1)^q (2K_q - p(a_q + b_q)), \tag{80}$$

$$A_q = (-1)^q (pc_q - K_q) : \frac{p-1}{2}. \tag{81}$$

Det første Udtryk viser, at Koefficienterne (mod. p) ere kongruente med Koefficienterne i $2(x-1)^{\frac{1}{2}(p-1)}$ eller, at

$$Y = 2(x-1)^{\frac{1}{2}(p-1)} + p(x^{\frac{1}{2}(p-3)} - \dots). \tag{82}$$

Her er det første Led paa højre Side for Mod. p kongruent med $+2$ eller -2, eftersom $x - 1$ er $R.$ eller $I.$ Altsaa:

Naar x er et helt Tal mindre end p, gaar p op i $Y - 2$ eller $Y + 2$, eftersom $x - 1$ er $R.$ eller $I.$ for p.

Sætte vi specielt $x = -1$, og erindre vi, at -2 er $R.$ for $p = 8n + 3$ og $I.$ for $p = 8n - 1$, og at Y for $x = -1$ maa have en af Værdierne $+2$ og -2, have vi:

For $x = -1$, bliver $Y = 2$ for $p = 8n + 3$, men $Y = -2$ for $p = 8n - 1$.

64. Vi kunne komme til det samme Resultat ad en anden Vej og derved tillige vinde en mærkelig Formel; sætte vi i

$$Y - \sqrt{-p}\,Z = 2\,\Pi(x - \varrho^r) \tag{83}$$

$x = -1$, faa vi

$$Y_{x=-1} = 2\,\Pi\left(-1 - \cos.\frac{2\pi r}{p} - \mathrm{i}\sin.\frac{2\pi r}{p}\right)^{*)}$$

$$= -2^{\frac{1}{2}(p+1)}\,\Pi\cos.\frac{\pi r}{p}\,\Pi\left(\cos.\frac{\pi r}{p} + \mathrm{i}\sin.\frac{\pi r}{p}\right)$$

$$= -2^{\frac{1}{2}(p+1)}\cos.\alpha\pi\,\Pi\cos.\frac{\pi r}{p} = (-1)^{\alpha+1}\,2^{\frac{1}{2}(p+1)}\,\Pi\cos.\frac{\pi r}{p}.$$

Her er Π positiv eller negativ, eftersom Antallet af Rester $> \frac{1}{2}p$ er lige eller ulige. Er $2 = R.$, er dette Antal α (28), og Fortegnet paa højre Side derfor $(-1)^{2\alpha+1} = -1$; er $2 = I.$, er Antallet $3\alpha - \frac{1}{2}(p-1)$ (29) og Fortegnet derfor bestemt ved $(-1)^{4\alpha - \frac{1}{2}(p-3)} = -1$, stemmende med Sætningen ovenfor.

Man faar nu tillige, naar 2 er $R.$, altsaa for $p = 8n - 1$

$$-2 = (-1)^{\alpha+1}\,2^{\frac{1}{2}(p+1)}\,\Pi\cos.\frac{\pi r}{p}$$

og for $p = 8n + 3$ modsat Fortegn paa venstre Side, saa at

$$\Pi\cos.\frac{\pi r}{p} = \pm\frac{1}{2^{\frac{1}{2}(p-1)}} \tag{84}$$

øverste Fortegn, naar $p = 8n - 1$, og α er lige eller, naar $p = 8n + 3$, og α er ulige, nederste Fortegn i de to andre Tilfælde.

---

*) At vi bruge Bogstavet i baade for Ikkerest og for $\sqrt{-1}$, kan ikke foraarsage Misforstaaelse.

Sætte vi i (83) $x = 1$, faa vi paa samme Maade

$$\sqrt{p}\, Z_{x=1} = (-1)^{\frac{1}{4}(p-3)}\, 2^{\frac{1}{2}(p+1)} \cos. \alpha\pi\, \Pi \sin. \frac{\pi r}{p},$$

hvor Π er positiv, da alle Vinklerne ere mindre end π.

Vi have set, at Z for $x = 1$ er $+2$ eller -2, og den fundne Formel viser, at Fortegnet ikke alene afhænger af, om 2 er *R.* eller *I.*, men ogsaa af, om α er lige eller ulige; derimod faa vi, uden Tvetydighed

$$\Pi \sin. \frac{\pi r}{p} = \frac{\sqrt{p}}{2^{\frac{1}{2}(p-1)}}. \tag{85}$$

65. Det andet Udtryk for Koefficienterne giver

$$\frac{1}{2}(p-1)\, Y = -(x-1)^{\frac{1}{2}(p-1)} + p\left(\Sigma (-1)^{q} c_q x^{\frac{1}{2}(p-1)-q}\right). \tag{86}$$

Da en Sum af to Rester ikke kan være p, har man $c_2 = 0$, hvorved den tredje Koefficient i Y bestemmes som $-\frac{p-3}{4}$.

For at bestemme a_q og b_q, skulle vi søge, paa hvor mange Maader q Rester kunne adderes saaledes, at Summen henholdsvis er en *R.* eller en *I.*; det er imidlertid tilstrækkeligt at søge Antallet af Summer, der ere kongruente med henholdsvis $+1$ og -1, da man ved at multiplicere de fundne Løsninger med alle *R.*, faar alle de Summer, der ere kongruente med henholdsvis alle *R.* og alle *I.* Altsaa:

Koefficienterne a_q, b_q og c_q ere henholdsvis lig Antallet af Løsninger af Kongruenserne (mod. p)

$$\Sigma r = +1;\ \Sigma r = -1;\ \Sigma r = 0, \tag{87}$$

hvor Σr betegner Summen af q Rester, og der for $+1$ og -1 kan sættes henholdsvis en vilkaarlig anden *R.* eller *I.*

Vi ville f. Eks. bestemme b_2; da Summen af to Rester er mindre end $2p$, skulle vi altsaa bestemme, paa hvor mange Maader $p-1$ kan deles i en Sum af to Rester. Lad os først antage, at 2 er *R.*, altsaa $p = 8n - 1$.

Vi fandt i 24, at for $p = 31$ vare de første Tal i Variationerne

$$\underset{\cdot}{2}\ 3\ \underset{\cdot}{5}\ \underset{\cdot}{6}\ \underset{\cdot}{10}\ 13\ \underset{\cdot}{14}\ 15\ \underset{\cdot}{16}\ 17\ \underset{\cdot}{20}\ 24\ \underset{\cdot}{25}\ 27\ \underset{\cdot}{28},$$

hvor de mærkede Tal ere Rester; vi saa, at disse forekom afvekslende med Ikkerester, og at Summen af to Tal, der staa lige langt fra det mellemste, er $p-1$; de to Addender blive her begge *R.* eller begge *I.* I den Række Tal, der bestaar af de første Tal i Permanenserne, have ogsaa to og to Summen $p-1$, men af de to Addender er den ene en *R.*, den anden en *I.* Vi have altsaa for Tallet 31 $b_2 = 4$. Sætte vi for 31 et vilkaarligt Primtal $8n-1$, bliver det midterste Tal $\frac{1}{2}(p-1)$, og dette Tal er en *I.*, da 2 er *R.* og -1 *I.* Foran det midterste Tal staar $\frac{1}{4}(p-3)$ Tal, og af disse er $\frac{1}{8}(p+1)$ Rester; man har altsaa $b_2 = \frac{1}{8}(p+1)$; er 2 *I.* for p, er det midterste Tal en *R.* og giver ikke nogen Løsning. Foran staa $\frac{1}{4}(p-3)$ Tal, af hvilke Halvdelen er Rester.

Man har altsaa

$$b_2 = \frac{1}{8}(p-3).$$

Da nu i begge Tilfælde ifølge (76)

$$a_2 + b_2 = \frac{1}{4}(p-3),$$

har man

$$(88)\quad \begin{cases} Y = 2x^{\frac{1}{2}(p-1)} + x^{\frac{1}{2}(p-3)} - \frac{1}{4}(p-3)x^{\frac{1}{2}(p-5)} + \dots \\ Z = x^{\frac{1}{2}(p-3)} + \begin{cases} 1 & 2 = R. \\ 0 & 2 = I. \end{cases} x^{\frac{1}{2}(p-5)} + \dots \end{cases}$$

Ved at indsætte disse Udtryk i

$$Y^2 + pZ^2 = 4\,(x^{p-1} + x^{p-2} + \dots + 1)$$

finder man den næste Koefficient i Y; den er

$$-\frac{1}{8}(3p-5), \text{ for } 2 = \mathrm{R},$$

$$\frac{1}{8}(p+5), \quad \text{for } 2 = I.$$

66. Af (76) følger, at hvis Tallet $\frac{1}{2}(p-1)$ gaar op i K_q, gaar det ogsaa op i c_q; dette Tilfælde indtræder som andetsteds vist, naar q er primisk med $\frac{1}{2}(p-1)$; vi kunne ogsaa indse dette saaledes:

Lad os antage, at vi have q Rester, hvis Sum er kongruent med Nul for Mod. p. Idet vi efterhaanden multiplicere med alle Resterne, faa vi $\frac{1}{2}(p-1)$ Løsninger af den sidste (87), hvis de alle ere forskellige.

Lad de Rester, der høre til en af Løsningerne, bestemmes ved Kongruensen

$$x^q + a_2 x^{q-2} + a_3 x^{q-3} + \ldots a_q \equiv 0, (\mathrm{mod.}\ p),$$

medens vi ved at multiplicere Resterne med en Rest r faa q Rester, som ogsaa give en Løsning, og som bestemmes ved

$$x^q + a_2 r^2 x^{q-2} + a_3 r^3 x^{q-3} \ldots + a_q r^q \equiv 0 \pmod{p}.$$

Hvis nu de to Løsninger falde sammen, maa man have

$$a_2(r^2-1) \equiv a_3(r^3-1) \ldots \equiv a_q(r^q-1) \equiv 0 \pmod{p}.$$

Her kan Produktet a_q af de q Rester ikke være deleligt med p, og man maa derfor have

$$r^q - 1 \equiv 0 \pmod{p},$$

hvad der er umuligt, hvis q er primisk med $\frac{1}{2}(p-1)$. Lad os derimod antage, at de to Tal have en fælles Faktor, og at r hører til Eksponenten e; da maa alle de Koefficienter være Nul, hvis Mærketal ikke ere delelige med e.

Lad os f. Eks. søge c_3 for $p = 19$. 3 gaar op i $\frac{1}{2}(p-1) = 9$, og Kongruensen

$$x^3 - 1 \equiv 0 \pmod{19}$$

giver Løsningen $1 + 7 + 11$, der bliver uforandret ved Multiplikation med 1, 7 og 11; de to andre Løsninger ere $4 + 6 + 9$ og $5 + 16 + 17$; var der et andet Sæt Løsninger, maatte disse indeholde enhver af Resterne tre Gange, og 1 maatte komme sammen med to Rester med Summen 18. Nu er imidlertid i den Række, der bestemmer Variationerne (1 3 7 8 9 10 11 15 17) $\frac{1}{4}(p+1) = 5$ Rester, og da $\frac{1}{2}(p-1)$ ikke kan benyttes, bliver der to Par Rester med Summen $p - 1 = 18$. Af disse kan $1 + 17$ ikke benyttes, da 1 ikke kan forekomme 2 Gange i Summen, og der er derfor kun et Par $(7 + 11)$, der kan benyttes. Der er derfor ikke flere Sæt Løsninger end det fundne.

Vi have derfor $c_3 = 3$ og Koefficienten A_3 for $p = 19$

$$(-1)^3 (57 - 84) : 9 = 3,$$

som vi fandt ovenfor ad anden Vej.

For c_4 faa vi, da 4 er primisk med 9, af een Løsning (f. Eks. $1 + 4 + 5 + 9$) dannet en Gruppe af 9 Løsninger, i hvilke hver Rest forekommer 4 Gange. Vi faa altsaa 4 Løsninger, der indeholde Tallet 1 og ved at borttage dette Tal 4 Løsninger, der høre til b_3; da der nu ogsaa er Løsninger, der indeholde Tallet 1 $(1 + 6 + 11)$, giver 1 Sæt Løsninger for c_4 mindst 5 Løsninger for b_3; da nu $a_3 + b_3 = 9$, kan der kun være 1 Sæt Løsninger for c_4, og man har derfor $c_4 = 9$, og, da $K_4 = 126$, Koefficienten

$$(-1)^4 (19 - 14) = 5.$$

67. Vi ville nu betragte $p = 23$, hvor vi af de fundne Koefficienter let udlede

$$a_1 = 1;\ b_1 = 0;\ c_1 = 0;\ a_2 = 2;\ b_2 = 3;\ c_2 = 0.$$

$\frac{1}{2}(p-1) = 11$ er primisk med alle q og gaar derfor op i alle K_q og c_q.

Betegnes Kvotienterne ved K_q' og c_q', have vi da

(89) $$a_q + b_q + c_q' = K_q'$$

og specielt

$$a_3 + b_3 + c_3' = 15,$$

hvor c_3' er Antallet af Sæt af Løsninger. I et saadant Sæt er der 3 (q) Løsninger med Leddet 1, og borttage vi dette, faa vi 3 Løsninger, hørende til b_2 og ikke indeholdende Tallet 1; da der nu i de b_2 Løsninger ikke er nogen med Leddet 1, have vi altsaa

$$3\,c_3' = b_2 = 3;\ c_3' = 1.$$

Den dertil svarende Koefficient er da

$$(-1)^3(23-15) = -8,$$

og endvidere er

$$a_3 + b_3 = 14.$$

Hvis c_4 indeholder c_4' Sæt Løsninger, vil der mellem disse være $4\,c_4'$, der indeholder Leddet 1, og hertil svare i b_3 lige saa mange Løsninger, der ikke indeholde Leddet 1, medens der er b_2 Løsninger, der indeholde 1. Vi have saaledes

$$b_3 = 4\,c_4' + b_2 = 4\,c_4' + 3.$$

c_4' kan ikke være Nul ($1 + 2 + 4 + 16 = 23$), og man maa derfor have enten

$$c_4' = 1;\ a_3 = b_3 = 7$$

eller

$$c_4' = 2;\ b_3 = 11;\ a_3 = 3.$$

Vi kunne imidlertid vise, at den sidste Løsning maa forkastes; der maa nemlig i a_3 være $b_2 = 3$ Løsninger, der indeholde Leddet 2 og $b_2 - 1$ Løsninger, der ikke indeholde Leddet 2, men Leddet 3. (Af de b_2 Løsninger af $r_1 + r_2 = 21$ maa $3 + 18$ forkastes).

Vi have saaledes fundet

$$c_4' = 1;\ a_3 = 7;\ b_3 = 7$$

og derved Koefficienten

$$(-1)^4 (23 - 30) = -7.$$

68. Vi kunne i Almindelighed danne Rekursionsformler, der dog komme til at afhænge af, hvilke af de første Tal, der ere Rester. Vi faa saaledes

$$b_7 = 8\,c_8' + b_6 - b_5 + b_4 - a_3 + b_2 - 1. \quad 7, -1;\ 6, -2;\ 5, -3;\ 4, -4;\ 3, -5;\ 2, -6;\ 1, -7.$$

$$b_8 = 9c'_9 + b_7 - b_6 + b_5 - a_4 + b_3 - a_2. \quad 8, -1;\ 7, -2;\ 6, -3;\ 5, -4;\ 4, -5;\ 3, -6;\ 2, -7;\ 1, -8.$$

Dette er at forstaa saaledes: I b_7 findes de Summer, der i $8\,c'_8$ indeholde 1, efter at dette Tal er subtraheret. De Led, der i b_7 indeholde 1, give, naar 1 subtraheres, Summer af 6 Rester, kongruente med -2 (*I.*), altsaa b_6, hvor dog de Summer, der indeholde 1, ikke ere med; disse give Summer af 5 Rester, kongruente med -3 (*I.*), altsaa b_5, hvor dog de, der indeholde 1, ikke ere med; disse give Summer af 4 Rester, kongruente med -4 (*I.*), altsaa b_4, hvor dog de, der indeholde 1, ikke ere med; disse give Summer af 3 Rester, kongruente med -5 (*R.*), altsaa a_3, hvor dog o. s. v.

Naar Summen af n Rester er kongruent med Nul, er Summen af de øvrige det ogsaa; man har derfor

$$c_n' = c'_{11-n},$$

ligesom

$$b_n = a_{11-n},$$

og de to Ligninger kunne derfor skrives

$$a_4 = 8\,c_3' + a_5 - b_5 + b_4 - a_3 + b_2 - 1 = a_5 - b_5 + b_4 + 3,$$
$$a_3 = 9\,c_2' + a_4 - a_5 + b_5 - a_4 + b_3 - a_2 = b_5 - a_5 + b_3 - 2,$$

hvoraf, da $a_3 = b_3$,

$$b_5 - a_5 = 2;\ b_4 - a_4 = -1,$$

og, da $c_4' = 1$, altsaa $a_4 + b_4 = 29$,

$$a_4 = 15;\ b_4 = 14,$$

og, da

$$b_4 = 5\,c_5' + b_3 - b_2,\ \text{altsaa}\ c_5' = 2;\ a_5 + b_5 = 40.$$
$$a_5 = 19;\ b_5 = 21.$$

For Koefficienten til x^6 faa vi da

$$(-1)^5\,(2 \cdot 23 - 42) = -4.$$

Den Ligning, der bestemmer Rødderne ϱ^r, er

$$Y - i\sqrt{p}\,Z = 0,$$

hvor de ovenfor fundne Værdier give:

p	Y
3	$2x + 1$
7	$2x^3 + x^2 - x - 2$
11	$2x^5 + x^4 - 2x^3 + 2x^2 - x - 2$
19	$2x^9 + x^8 - 4x^7 + 3x^6 + 5x^5 - 5x^4 - 3x^3 + 4x^2 - x - 2$
23	$2x^{11} + x^{10} - 5x^9 - 8x^8 - 7x^7 - 4x^6 + 4x^5 + 7x^4 + 8x^3 + 5x^2 - x - 2$

p	Z
3	1
7	$x^2 + x$
11	$x^4 + x$
19	$x^8 - x^6 + x^5 + x^4 - x^3 + x$
23	$x^{10} + x^9 - x^7 - 2x^6 - 2x^5 - x^4 + x^2 + x$

Disse Resultater ere de samme, som ere fundne af *Gauss* ved Hjælp af Røddernes Potenssummer.

II. VISSE SYMMETRISKE FUNKTIONER AF RESTERNE.

69. Idet vi sætte

$$Y^2 + pZ^2 = u = 4\frac{x^p - 1}{x - 1},$$

have vi

$$(x - 1)u = 4(x^p - 1),$$

hvoraf ved Differentiation udledes Ligningerne

$$(x - 1)u' + u = 4px^{p-1},$$
$$(x - 1)u'' + 2u' = 4p(p - 1)x^{p-2},$$
$$(x - 1)u''' + 3u'' = 4p(p - 1)(p - 2)x^{p-3} \text{ o. s. v.}$$

Sætte vi $x = 1$, faa vi af den første Ligning

$$Y_{x=1} = 0; \; Z^2_{x=1} = 4.$$

Z har altsaa for $x = 1$ den numeriske Værdi 2, og vi se af 64, at Fortegnet bestemmes af

$$(-1)^{\frac{p-3}{4}} \cos. \alpha\pi, \; (\Sigma r = \alpha p),$$

saa at

$$Z_{x=1} = (-1)^{\alpha + \frac{p-3}{4}} . 2. \tag{90}$$

Af den anden Ligning faa vi

$$(ZZ')_{x=1} = p - 1, \tag{91}$$

saa at Z' for $x = 1$ har den numeriske Værdi $\frac{1}{2}(p - 1)$ og det samme Fortegn som Z.

Af den tredje Ligning faar man

$$(Y'^2 + pZZ'')_{x=1} = \frac{1}{12}p(p - 1)(5p - 13),$$

hvoraf da, som vi straks ville finde,

$$Y'^2_{x=1} = p^2(\beta - \alpha)^2,$$

$$(ZZ'')_{x=1} = \frac{1}{12}(p - 1)(5p - 13) - p(\beta - \alpha)^2.$$

70. Af $u = 0$ finder man for $x = -1$

$$Z = 0;\ Y = \pm 2.$$

Fortegnet kan her bestemmes, som vi have vist i 63, hvor vi fandt, at det er $+$ for $p = 8n + 3$, $-$ for $p = 8n - 1$. Af den første Ligning faar man

$$(YY')_{x=-1} = -(p-1), \tag{92}$$

altsaa

$$Y'_{x=-1} = \mp \frac{1}{2}(p-1),$$

øverste Fortegn for $p = 8n + 3$, nederste for $p = 8n - 1$.

71. Anvende vi den bekendte Formel

$$\frac{xf'(x)}{f(x)} = n + \frac{s_1}{x} + \frac{s_2}{x^2} + \ldots \quad (x > 1) \tag{93}$$

paa Ligningen

$$Y - i\sqrt{p}\,Z = 0,$$

have vi $s_q = y_1$, hvis q er $R.$, men $s_q = y_2$, hvis q er $I.$ og derfor

$$x\,\frac{Y' - i\sqrt{p}\,Z'}{Y - i\sqrt{p}\,Z} = \frac{1}{2}(p-1) + \frac{y_1}{x} + \ldots + \frac{y_1}{x^r} \ldots + \frac{y_2}{x^i} + \ldots$$

$$= \frac{1}{2}(p-1) + \left(\frac{y_1}{x} + \ldots + \frac{y_2}{x^{p-1}}\right)\left(1 + \frac{1}{x^p} + \frac{1}{x^{2p}} + \ldots\right)$$

$$(p = 4n + 3),$$

$$= \frac{x^p}{x^p - 1}\left(\frac{1}{2}(p-1) + y_1 \sum \frac{1}{x^r} + y_2 \sum \frac{1}{x^i}\right),$$

(r og i mindre end p),

hvoraf

$$\frac{1}{4}x(x-1)(Y' - i\sqrt{p}\,Z')(Y + i\sqrt{p}\,Z) = \frac{1}{2}(p-1)x^p + y_1 \Sigma x^i + y_2 \Sigma x^r,$$

eller, idet vi skille Reelt og Imaginært,

$$\frac{1}{2}(x-1)(YY' + pZZ') = px^{p-1} - \frac{x^p - 1}{x - 1}. \tag{94}$$

(95) $$\frac{1}{2}x(x-1)(YZ'-ZY') = \Sigma x^r - \Sigma x^i,$$

hvor den første Ligning ogsaa faas direkte ved Differentiation af (79).

Af Ligning (95) faa vi, idet vi dividere med $x-1$ og sætte $x=1$,

(96) $$(ZY')_{x=1} = 2p(\beta-\alpha),$$

hvoraf

(97) $$Y'_{x=1} = (-1)^{\alpha+\frac{p-3}{4}}(\beta-\alpha)p,$$

og ved at differentiere Ligningen

$$(x-1)(YZ'-ZY') = 2\Sigma(x^{r-1}-x^{i-1})$$

to Gange.

(98) $$(ZY'')_{x=1} = p(p-3)(\beta-\alpha).$$

For $x=-1$, faa vi af (95)

$$(YZ')_{x=-1} = r_l - r_u - i_l + i_u = 2(r_l - r_u) = \begin{cases} 2(\beta-\alpha) \text{ for } p=8n-1 \\ 6(\alpha-\beta) \text{ for } p=8n+3, \end{cases}$$

altsaa

(99) $Z'_{x=-1} = \alpha-\beta$ for $p=8n-1$ og $3(\alpha-\beta)$ for $p=8n+3$.

Ved Differentiation af (95), faa vi for $x=-1$

$$Y(Z''-\frac{1}{2}Z') = \Sigma(r_u - r_l - i_u + i_l) = \alpha p - 2\Sigma r_l - \beta p + 2\Sigma i_l.$$

Nu er (28) for $p=8n-1$ i Tallenes første Halvdel Summen af Resterne lig Summen af Ikkeresterne, medens for $p=8n+3$ for Tallenes første Halvdel

$$\Sigma r - \Sigma i = (\beta-\alpha)p \quad (29),$$

og vi faa derfor paa højre Side i de to Tilfælde henholdsvis

$$(\alpha-\beta)p \text{ og } 3(\beta-\alpha)p,$$

og deraf for $x = -1$

$$(100)\qquad \begin{aligned} Z'' &= \frac{1}{2}(p-3)(\beta-\alpha) \quad p = 8n-1, \\ Z'' &= \frac{3}{2}(p-3)(\beta-\alpha) \quad p = 8n+3. \end{aligned}$$

De fundne Resultater samles i følgende Tabel:

$x = 1.\ \ \alpha + \frac{p-3}{4} = \xi;$	$x = -1.$
$Y = 0;$	$Y = \mp 2;\ \begin{cases} p = 8n-1. \\ p = 8n+3. \end{cases}$
$Z = (-1)^{\xi}.2;$	$Z = 0.$
$Y' = (-1)^{\xi}(\beta-\alpha)\ p;$	$Y' = \pm\frac{1}{2}(p-1);\ \begin{cases} p = 8n-1. \\ p = 8n+3. \end{cases}$
$Z' = (-1)^{\xi}\frac{1}{2}(p-1);$	$Z' = \begin{cases} \alpha-\beta; & p = 8n-1. \\ 3(\alpha-\beta); & p = 8n+3. \end{cases}$
$Y'' = (-1)^{\xi}p(p-3)(\beta-\alpha);$	$Y'' = \begin{cases} \frac{1}{2}p(\beta-\alpha)^2 - \frac{3}{8}(p-1)^2; & p=8n-1. \\ -\frac{9}{2}p(\beta-\alpha)^2 + \frac{3}{8}(p-1)^2; & p=8n+3. \end{cases}$
$\begin{cases} Z'' = (-1)^{\xi}\cdot\frac{1}{24}(p-1) \\ (5p-13) - \frac{1}{2}p(\beta-\alpha)^2; \end{cases}$	$Z'' = \begin{cases} \frac{1}{2} \\ \frac{3}{2} \end{cases}(p-3)\ (\beta-\alpha);\ p = \begin{cases} 8n-1. \\ 8n+3. \end{cases}$

71. Man har som bekendt ved Rækkeudvikling

$$\frac{Y' - i\sqrt{p}Z}{Y - i\sqrt{p}Z} = \sum\frac{1}{x-\varrho^r} = \sum\frac{1}{x} + y_1\sum\frac{1}{x^{r+1}} + y_2\sum\frac{1}{x^{i+1}}.\quad x>1.$$

Ombytter man her i med $-i$, bliver den reelle Del uforandret, medens den imaginære Del skifter Tegn; man har derfor

$$(101)\qquad \begin{aligned} \sum\left(\frac{1}{x-\varrho^r} - \frac{1}{x-\varrho^i}\right) &= 2i\sqrt{p}\,\frac{ZY' - YZ'}{Y^2 + pZ^2} \\ &= i\sqrt{p}\sum_1^{\infty}\left(\frac{1}{x^{r+1}} - \frac{1}{x^{i+1}}\right), \quad x > 1 \end{aligned}$$

hvor

$$(102)\qquad \sum\left(\frac{1}{x-\varrho^r}-\frac{1}{x-\varrho^i}\right)=2i\sum\frac{\sin.\frac{2\pi r}{p}}{x^2-2\cos.\frac{2\pi r}{p}x+1},$$

og ifølge (95)

$$(103)\qquad 2i\sqrt{p}\,\frac{ZY'-YZ'}{Y^2+pZ^2}=-i\sqrt{p}\sum\frac{x^r-x^i}{x(x^p-1)}.$$

Af (102) og (103) følger for $x=0$

$$(104)\ \Sigma(\varrho^r-\varrho^i)=2i\sum\sin.\frac{2\pi r}{p}=y_1-y_2=+i\sqrt{p},\ (74)$$

altsaa

$$(105)\qquad \sum\sin.\frac{2\pi r}{p}=\frac{1}{2}\sqrt{p}.$$

For $x=1$ faar man

$$\sum\left(\frac{1}{1-\varrho^r}-\frac{1}{1-\varrho^i}\right)=i\sum\cot.\frac{\pi r}{p}=i\sqrt{p}\,(\beta-\alpha),\ (\text{Tab. Pag. 72}),$$

følgelig

$$(106)\qquad \sum\cot.\frac{\pi r}{p}=\sqrt{p}\,(\beta-\alpha).$$

For $x=-1$ faar man

$$-\sum\left(\frac{1}{1+\varrho^r}-\frac{1}{1+\varrho^i}\right)=i\sum\text{tg.}\frac{\pi r}{p}=-i\sqrt{p}\,(\beta-\alpha)(p=8n-1)$$

$$\text{og}\quad 3i\sqrt{p}\,(\beta-\alpha)\,(p=8n+3)$$

og følgelig

$$(107)\sum\text{tg.}\frac{\pi r}{p}=-(\beta-\alpha)\sqrt{p}\,(p=8n-1)\,\text{og}=3(\beta-\alpha)\sqrt{p}\ \ (p=8n+3).$$

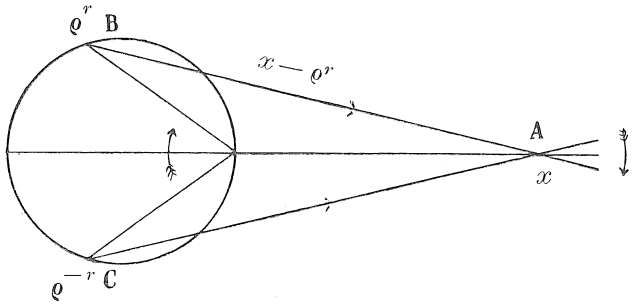
72. Af Ligningen

$$\sum\left(\frac{1}{x-\varrho^r}-\frac{1}{x-\varrho^i}\right)=i\sqrt{p}\sum_1^\infty\left(\frac{1}{x^{r+1}}-\frac{1}{x^{i+1}}\right)\ x>1$$

faa vi, naar vi multiplicere med dx og integrere langs med de reelle Tals Akse fra ∞ til 1

$$\sum \mathrm{l}.\frac{1-\varrho^{r}}{1-\varrho^{-r}} = -i\sqrt{p}\sum\left(\frac{1}{r}-\frac{1}{i}\right), \tag{108}$$

idet den uendelige Række, vi faa ved Integrationen, ogsaa er konvergent for $x = 1$. Den har i Nævnerne alle positive hele Tal undtagen de, der ere Multipla af p.



For nærmere at bestemme Logaritmen, ville vi betegne de Punkter paa Enhedscirklen, der svare til ϱ^{r} og ϱ^{-r}, ved B og C, medens A betegner Punktet x, liggende mellem 1 og ∞. Brøkens Argument er da Vinklen fra CA til BA; denne er Nul for $x = \infty$, medens den for $x = 1$ er

$$-\left(\pi-\frac{2\pi r}{p}\right),$$

som derfor er Argumentets Tilvækst, naar x gaar ∞ til 1. Summere vi for alle Resterne, faa vi da Integralets Værdi

$$-\left(\frac{p-1}{2}\pi-\frac{2\pi\alpha p}{p}\right)i = -\pi(\beta+\alpha-2\alpha)i = -\pi(\beta-\alpha)i$$

og saaledes

$$\pi(\beta-\alpha) = \sqrt{p}\sum\left(\frac{1}{r}-\frac{1}{i}\right). \tag{109}$$

Summen danner en betinget konvergent Række, hvor stadig de $p-1$ Led tages sammen, hvis Nævnere ligge mellem to paa hinanden følgende Multipla af p.

For nærmere at bestemme Summen erindre vi om *Eulers* bekendte Formel

$$\Pi \frac{1}{1-p^{-z}} = 1 + \frac{1}{2^z} + \frac{1}{3^z} + \frac{1}{4^z} + \ldots,$$

hvor Produktet dannes, idet der efterhaanden for p sættes alle Primtal. Her gøre vi imidlertid den Ændring, at vi udelade alle Multipla af det Primtal p, vi ovenfor have tænkt os givet, og for et andet Primtal q tage Fortegnet i Nævneren som + eller —, eftersom q er *R.* eller *I.* for p; i Rækken faa da Leddene + eller —, eftersom de hele Tal i Nævneren indeholde et lige eller ulige Antal Primfaktorer, der ere Ikkerester for p, det vil sige, eftersom det hele Tal selv er *R.* eller *I.* for p. Ændringen medfører, at medens Eulers Formel kun gælder, naar den reelle Del af z er større end 1, gælder den ændrede Formel for den reelle Del positiv og derfor for $z=1$, saa at man har

$$\pi(\beta - \alpha) = \sqrt{p} \sum \left(\frac{1}{r} - \frac{1}{i}\right) = \sqrt{p}\, \Pi \frac{1}{1 \mp q^{-1}}$$

altsaa, da alle Produktets Faktorer ere positive,

$$\beta > \alpha. \tag{110}$$

Vi have saaledes faaet et direkte Bevis for denne Sætning og derved set, at den staar i nær Forbindelse med Gauss's Fortegnssætning, der er benyttet ved Beviset.

III. ALTERNERENDE FUNKTIONER AF ENHEDSRØDDERNE.

73. Vi have betragtet flere alternerende Funktioner af de komplekse Enhedsrødder. Ifølge Ligningernes Teori kunne disse Funktioner alle udtrykkes rationalt ved Kvadratroden af

den irreduktible Lignings Diskreminant, altsaa i det her betragtede Tilfælde ifølge (57) ved $\sqrt{-p}$. En saadan Funktion er

$$\Pi(\varrho^r - \varrho^{-r}) = (2i)^{\frac{1}{2}(p-1)} \Pi \sin. \frac{2\pi r}{p},$$

hvor, ifølge (84) og (85)

$$\Pi \sin. \frac{2\pi r}{p} = \pm 2^{\frac{p-1}{2}} \frac{\sqrt{p}}{2^{p-1}},$$

altsaa

$$\Pi(\varrho^r - \varrho^{-r}) = \pm i^{\frac{1}{2}(p-1)} \sqrt{p} = \pm i\sqrt{p}, \tag{111}$$

hvor, idet Potensen af i er $-i$ eller $+i$, eftersom $p = 8n-1$ eller $p = 8n+3$, Fortegnsbestemmelsen ved (84) viser, at man kan sætte

$$\Pi(\varrho^r - \varrho^{-r}) = (-1)^{\beta} i\sqrt{p}.$$

Vi have her den samme Vanskelighed ved Bestemmelsen af Fortegnet, som vi have truffet ved andre alternerende Funktioner, som afhænge af Resternes Fordeling. Vi kunne imidlertid benytte det fundne Resultat til at bestemme en anden alternerende Funktion, hvor Fortegnet let bestemmes, og opnaa dette, naar vi i Stedet for Eksponenterne r sætte de ulige Tal $1, 3, 5, \ldots p-2$; derved forandres den numeriske Værdi ikke, medens saa mange af Faktorerne, som der er lige Rester, skifte Tegn. Dette Antal er β for $p = 8n-1$ og $3\alpha - \frac{1}{2}(p-1)$ for $p = 8n+3$; da dette Tal er lige eller ulige samtidig med β, faa vi da i alle Tilfælde

$$P = (\varrho - \varrho^{-1})(\varrho^3 - \varrho^{-3})(\varrho^5 - \varrho^{-5}) \ldots (\varrho^{p-2} - \varrho^{-(p-2)}) = i\sqrt{p}.$$

Vi have her udledt denne Formel ad en Omvej, men kunne ogsaa danne den direkte og det paa saadan en Maade, at vi ikke dertil benytte Gauss's Fortegnssætning; vi faa nemlig, idet vi i P tage Faktorerne i omvendt Orden og med modsatte Fortegn,

$$-P = (\varrho^2 - \varrho^{-2})(\varrho^4 - \varrho^{-4}) \ldots (\varrho^{p-1} - \varrho^{-(p-1)})$$

og ved Multiplikation af de to Ligninger og Divisjon med

$$\varrho^{1+2+3+\ldots+(p-1)} = 1$$

$$-P^2 = (1-\varrho^{-2})(1-\varrho^{-4})\ldots = (1-\varrho)(1-\varrho^2)(1-\varrho^3)\ldots(1-\varrho^{p-1}) = p,$$

altsaa

$$P = \pm i\sqrt{p},$$

hvor Fortegnet bestemmes ved

$$(2i)^{\frac{1}{2}(p-1)} \Pi \sin.(2n+1)\frac{2\pi}{p}. \quad 2n+1 = 1, 3, 5 \ldots p-2.$$

Her er der i Produktet $\frac{1}{4}(p-3)$ negative sin., altsaa et ulige Antal for $p = 8n-1$, et lige Antal for $p = 8n+3$; sammenholdes dette med, at Potensen af i i de to Tilfælde er henholdsvis $-i$ og $+i$, faa vi som før

$$P = +i\sqrt{p}.$$

P har ligesom

$$S = \Sigma(\varrho^r - \varrho^{-r})$$

den Egenskab at blive uforandret, naar vi for ϱ sætte ϱ^r, men skifte Tegn, naar vi for ϱ sætte ϱ^{-r}, og man har derfor for alle de komplekse Enhedsrødder*), og, som man straks ser, ogsaa naar vi for ϱ sætte 1,

$$S = P.$$

Heraf følger, hvis vi sætte

$$S(x) = \Sigma(x^r - x^{p-r})$$

$$P(x) = (x - x^{p-1})(x^3 - x^{p-3})\ldots(x^{p-2} - x^2),$$

at Ligningen

(112) $$S(x) - P(x) = 0$$

---

*) Se ogsaa Kronecker: Liouvilles Journal Bd. 1, 2den Serie.

er tilfredsstillet af alle Rødder af $x^p - 1 = 0$, og at derfor dens venstre Side er delelig med $x^p - 1$. Da nu $S(x)$ ikke har nogen Eksponent større end $p - 1$, kan dette ogsaa udtrykkes saaledes, at $S(x)$ netop bliver Resten, naar $P(x)$ divideres med $x^p - 1$, eller at vi netop faa $S(x)$, naar vi udføre Multiplikationerne i $P(x)$ og for hver Eksponent sætte dens laveste positive Rest for Divisor p.

Her er det forudsat, at den Gauss'iske Fortegnssætning er kendt; er dette ikke Tilfældet, vide vi ikke, med hvilket Fortegn vi skulle tage $P(x)$ i Ligningen (112). Dersom vi derfor kunne vise, at Divisjonsresten bliver $S(x)$, have vi et Bevis for Fortegnssætningen, ja, det vil være tilstrækkeligt at vise, at et af Leddene passer, f. Eks. at Leddet x i Resten faar Koefficienten 1.

Vi kunne ogsaa i Stedet for Leddet med Eksponenten 1 tage Leddet med Eksponenten $1 + 3 + 5 + \ldots + p - 2$, da denne Sum som bekendt er et Kvadrattal. De dermed kongruente Summer maa have de samme Led, kun at nogle af dem ere negative; disses Sum maa være kongruent med Nul, og der maa mellem Summerne være lige mange, der have et lige Antal, og der have et ulige Antal Addender. Disse Summer forekomme som Eksponenter i det udviklede Produkt

$$(1 - x)(1 - x^3)(1 - x^5)\ldots(1 - x^{p-2}).$$

Man kan altsaa af den Gauss'iske Fortegnssætning udlede følgende mærkelige Sætning om Primtallene:

Dersom de forskellige Multipla af et Primtal p skrives som Summer af forskellige ulige Tal, tagne mellem Tallene $1, 3, 5 \ldots p - 2$, vil Antallene af Maader, hvorpaa dette kan gøres, være ens for de ulige og for de lige Multipla.

Saaledes have vi f. Eks. for $p = 11$, hvor den størst mulige Sum er 25,

$$11 = 1 + 3 + 7;\ 22 = 1 + 5 + 7 + 9.$$

Paa den anden Side vilde et direkte Bevis for denne Sætning straks føre til Fortegnssætningen; et saadant Bevis er det imidlertid, trods store Anstrængelser, ikke lykkedes mig at føre.

74. Dersom vi dividere $P(x) - S(x)$ med $x^p - 1$ og dekomponere Brøken, faa vi, idet ϱ er et vilkaarligt af Nævnerens komplekse Nulpunkter,

$$(113)\quad \frac{\Sigma x^r - \Sigma x^i}{x^p - 1} = \sum \frac{(\varrho - \varrho^{p-1})(\varrho^3 - \varrho^{p-3}) \ldots (\varrho^{p-2} - \varrho^2)}{p\varrho^{p-1}(x - \varrho)}.$$

Vi multiplicere denne Ligning med $x^p - 1$, differentiere og sætte $x = 1$, hvorved vi faa

$$(\alpha - \beta)p = \sum \frac{(\varrho - \varrho^{p-1})(\varrho^3 - \varrho^{p-3}) \ldots}{\varrho^{p-1}(1 - \varrho)}$$

$$= (-1)^{\frac{p-3}{4}} \Sigma p^{\frac{p^2+7}{8}} (1 - \varrho^3)(1 - \varrho^5)(1 - \varrho^7) \ldots (1 - \varrho^{p-2}).$$

Idet vi her udføre Multiplikationen i sidste Led og addere, falde alle de Led bort, hvis Eksponenter ikke ere delelige med p, medens de andre give $\pm p$, nemlig $+$ for de Led, hvor Antallet af Addender i Eksponenten er lige, $-$, hvor det er ulige, altsaa

$$\alpha - \beta = k - l,$$

hvor k og l henholdsvis betyde Antallet af Maader, paa hvilke $\frac{p^2+7}{8}$ kan sættes $\equiv$ med en Sum af et lige eller et ulige Antal af forskellige Addender, tagne mellem Tallene $3, 5, 7 \ldots p-2$.

Saaledes for $p = 19$ faa vi, at de Tal, der skulle opløses, ere 11, 30, 49 og 68, der give 6 lige Opløsninger, nemlig $17+13$, $3 + 7 + 9 + 11$ o. s. v. og 7 ulige, nemlig $11, 17 + 15 + 9 + 5 + 3$ o. s. v., saa at $\alpha - \beta = 6-7$; $\beta - \alpha = 1$; $\beta + \alpha = 9$; $\beta = 5$; $\alpha = 4$.

Dersom man multiplicerer $S(x)$ med x og gaar frem som ovenfor, faar man paa venstre Side ikke Polynomiets Rest for

Divisor $x^p - 1$, da et af Leddene bliver $-x^p$ (da -1 er *I.*), der maa forandres til $-x^0$, naar vi paa venstre Side ville have Divisjonsresten. Da nu $\Sigma(r+1) - \Sigma(i+1) = (\alpha - \beta)p$, bliver venstre Side nu $(\alpha - \beta + 1)p$. Havde $p-1$ været en *R.*, vilde vi have faaet $(\alpha - \beta - 1)p$. Paa højre Side er der under Tegnet Σ kommen en Faktor ϱ til.

Ved det reducerede Produkt ville vi forstaa det Polynomium, som dannes ved Multiplikationen, idet vi sætte $\varrho^k = \varrho^{k+p} = \varrho^{k+2p} \ldots = x^k$. I Polynomiet er en af Koefficienterne $\pm(\beta - \alpha)$ og de følgende vokse altsaa 1, hver Gang vi passere en *R.* og aftage med 1, naar man passerer en *I.* Saaledes for $p=11$ faa vi

$$\varrho^5(1-\varrho^3)(1-\varrho^5)(1-\varrho^7)(1-\varrho^9),$$

der giver Polynomiet

$$x^{11} + 0 \cdot x^{10} + x^9 + 0 \cdot x^8 - x^7 - 2x^6 - x^5 + 0x^4 + x^3 + 0x^2 + x,$$

hvor den første Koefficient er $\beta - \alpha = 1$, den anden 0, (10 = *I.*), den næste 1, (9 = *R.*), den næste 0, (8 = *I.*) o. s. v.

I Rektoratsaaret 1906—1907 have 13 Videnskabsmænd opnaaet akademiske Grader, nemlig 5 den medicinske og 8 den filosofiske Doktorgrad. De af dem meddelte Oplysninger om deres Livsforhold og Studier aftrykkes her i den Orden, hvori de have vundet Graden.

I.

Jeg, Knud Frederik Krog Fabricius, født i Aarhus $^{13}/_{8}$ 1875, er Søn af Historikeren, Pastor Adam Kristoffer Fabricius (1822—1902) og Hustru Nikoline Frederikke f. Jensen. Min Opvækst foregik i Holme Præstegaard, hvor jeg, samtidig med at en levende Kærlighed til Danmarks Historie vaktes hos mig, modtog et stærkt og pinligt Indtryk af Provisorietidens Evne til at spalte Befolkningen. Mine Skoleaar tilbragte jeg i Aarhus Latinskole og i Metropolitanskolen, hvor Datidens Mangel paa Evne til at vække Interessen hos Eleverne og til at udvikle deres Personlighed, undertiden forbundet med en ligefrem Dekadence, bidrog sit til at gøre mig til en sløv og forkuet Skoledreng. Det var derfor en Lykke for mig, at jeg i 1891—1892 fik et Aars Hviletid under Apoteksvirksomhed, inden jeg i 1895 tog Artium fra H. Cohns Kursus i København. Resultatet blev ganske vist kun 2den Karakter, men jeg mindes altid med Glæde mine dygtige Lærere ved dette Kursus, blandt hvilke jeg navnlig maa takke cand. mag. Vincens Strøm, min første virkelige Historielærer. Ved Universitetet blev jeg navnlig paavirket af Høffdings Forelæsninger (Filosofikum i 1896 med Udmærkelse) og af Erslevs og Steenstrups Historieundervisning, der førte mig ind i vor Middel-

aldersforskning; (min første Specialafhandling „Bondeoprøret 1441" udkom i Historisk Tidsskrift i 1900). Ikke mindst har Erslev gennem sin stadige Interesse for mig og mit Arbejde bidraget væsentlig til at udvikle mig og givet mig Mod til at tage fat paa en Række Opgaver. Ligeledes voksede min Hengivenhed for engelsk Kultur (allerede vakt i Drengeaarene gennem Scott), og jeg blev sat i Stand til at tilbringe to Sommermaaneder i 1900 under Sprogstudier i England og Skotland. Endelig vaktes nu først for Alvor min Lyst til Verdenshistorien gennem Læsning af Ranke, der blev min historiske Yndlingsforfatter. I Januar 1901 tog jeg da Embedseksamen med Laudabilis (Historie, Engelsk og Latin). Den nærmeste Tid herefter viede jeg til fortsat Arbejde i vor Middelaldershistorie, og jeg har offentliggjort en Række Afhandlinger derover („Den jydske Krig i Efteraaret 1157" i Hist. Tidsskr. VII, 3.; „En nordisk Lensmands Liv i det 15de Aarhundrede" i Svensk hist. Tidskr. 1904 (om Iver Akselsøn); og „Gotlandske Forhold under Iver Akselsøn Tot" i Antikvarisk Tidskrift för Sverige XVII, 5). Samtidigt vendtes dog ogsaa mit Blik mere og mere mod nyere Tider, og det fæstede sig navnlig ved vor ældre Enevældes Tidsrum. Til at komme ind paa et saadant Studium af dansk—svensk Historie 1660—1720 lededes jeg desuden derigennem, at jeg allerede fra mine første Studenteraar havde faaet Lyst til en Gang at undersøge det skaanske Nationalitetsskiftes Historie nærmere. Den ydre Anledning hertil kom ved Universitetets Prisopgave 1901—1902. Besvarelsen heraf indbragte mig Medaljen, og jeg fik snart efter Rejselegater til et mere dybtgaaende Studium over Emnet i Udlandet. Saaledes blev det mig muligt at tilbringe Tiden mellem Decbr. 1903 og Sommeren 1907 i det væsentlige uden for Danmark. Indtil Sommeren 1906 arbejdede jeg i Sverige og Tyskland, hvor jeg bl. a. var Student i Lund og i Berlin; 1906—1907 rejste jeg i Østrig, Italien, Nordafrika og Spanien. Foruden de to første Dele af Arbejdet „Skaanes Overgang fra Danmark til Sverige", der gaa til 1676, og af hvilke jeg forsvarede den anden („Den skaanske Provins") for den filosofiske Doktorgrad ved vort Universitet i Novbr. 1906, blev Frugten af Rejsen

dels en Indtrængen i de forskellige Landes Aandsliv, dels en (delvis) Indsamling af det Stof til Danmarks Historie i det 17de Aarh.s sidste Halvdel, som jeg i saa rigt Maal fandt i udenlandske Arkiver (Berlin, Marburg, Dresden, Wien, Venezia og Simancas).

Jeg arbejdede før min Bortrejse som Lærer ved forskellige københavnske Skoler, og har nu atter genoptaget denne Virksomhed. Desuden deltager jeg i Folkeuniversitetsgerningen og er Volontør i Rigsarkivet. 1901—1903 var jeg historisk Anmelder ved „Dannebrog" og deltog bl. a. i den berømmelige Nils Kjeldsens Fejde. Derhos har jeg skrevet Rejsebreve fra England i 1900 i „Vort Land" og fra Nordafrika og Spanien i 1907 i „Berlingske Tidende". I 1903 var jeg $^1/_2$ Aar Senior i Studenterforeningen.

Jeg ægtede $^{19}/_5$ 1906 i Norrköping Estrid Stolpe, Datter af afdøde Intendent ved Riksmuseums etnografiske Afdeling i Stockholm, Prof. Hj. Stolpe og hans Hustru Emmy født Holmgren.

II.

Adam Giede Bøving, født i Sæby Købstad 31. Juli 1869. Tilhører en Slægt, som i lige Linje stammer fra en Købmand og Raadsherre i Hattingen i Tyskland Henrik B. (død 1625) og som i Danmark lader sig føre tilbage til Johan Georg B., 1708 Missionær i Trankebar, senere Præst i København og tillige ethnografisk Forfatter. Min Fader er nuværende Præst i Barløse paa Fyen Niels Orten Mathias B.; min Moder, Ottilia Louisa Augusta f. Giede, døde 1898.

Jeg blev Student 1888 fra Aalborg Kathedralskole (1ste K.), tog Filosofikum 1889 (ug.) og Magisterkonferents i Naturhistorie Foraaret 1894. Derefter Lærer. Ansattes 1902 ved zoologisk Museums 3die Afdeling. Forsvarede d. 17. Dec. 1906 for den filosofiske Doktorgrad en Afhandling om Donaciinlarvernes Naturhistorie. Ægtede 3die Nov. 1903 cand. phil. Poula Margrethe Brønnum, Datter af afdøde Fabrikant Ludvig Br., Christianshavns Jærnstøberi og Hustru Henriette født Giede.

III.

Carl Emil Hansen Ostenfeld, Søn af fhv. Stiftsfysikus Carl Emil Hansen og Hustru Karen Marie Ostenfeld, er født i Randers d. 3. August 1873. Tog i 1889 4de Klasses Hovedexamen ved Randers lærde Skole og flyttede samme Sommer til Nykøbing F., hvor min Fader da var bleven Stiftsfysikus; herfra tog jeg i 1891 Examen Artium (I. Kar.). I 1892 Filosofikum (I. Kar.) og i 1893 den lægevidenskabelige Forberedelsesexamen med Udvidelse i Fysik og Kemi samt i Forsomren 1897 Magisterkonferens i Naturhistorie med Botanik som Hovedfag.

Da jeg fra Barnsben har haft levende Interesse for Naturvidenskab og, allerede før jeg blev Student, havde erhvervet mig en betydelig Kendskab til den danske Flora, faldt det af sig selv, at jeg studerede de biologiske Fag, særlig Botanik under Professor Dr. E. Warmings fortræffelige Vejledning. Fra min Studietid mindes jeg iøvrigt med Glæde Undervisningen hos Professor Dr. C. Lütken og Professor Rasmus Pedersen.

I Somrene 1895 og 1896 deltog jeg som Botaniker i den danske Ingolf-Expedition til Havene omkring Island og Grønland og kom derved ind paa Studiet af Plankton, særlig Havets Planteplankton; for at sætte mig mere ind i dette interessante Studium opholdt jeg mig i Efteraaret 1896 en kort Tid hos Professor Dr. P. T. Cleve i Upsala.

I 1897 berejste jeg i Selskab med cand. pharm. J. Hartz Færøerne for at studere Øernes Flora og Vegetation. Næste Aar (1898) tilbragte jeg en Del Tid paa den danske biologiske Station hos Dr. C. G. Joh. Petersen, hos hvem jeg i 1900 var Assistent. I Efteraaret 1900 ansattes jeg som Museumsinspektør ved Universitetets botaniske Haves Museum, hvor jeg forinden havde haft Arbejde som Extrahjælper. Samme Aar var jeg bleven Medlem af Kommissionen for Havundersøgelser og overtog i 1902 Ledelsen af Planktonundersøgelserne ved de da begyndende internationale Havundersøgelsers danske Afdeling.

Af Studierejser udover de ovenfor nævnte til nordlige Lande har jeg — hovedsagelig i Museumsøjemed og med Understøttelse fra forskellig Kant — foretaget kortere Besøg i

London, Amsterdam, Wien, Berlin, St. Peterborg, Helsingfors og Stockholm.

Med Understøttelse fra Carlsbergfondet arbejdede jeg i 1899—1901 sammen med min afdøde Ven, cand. pharm. O. Gelert paa en Haandbog i den arktiske Flora, hvoraf første Del udkom i 1902 med Titlen „Flora Arctica", I. I Samarbejde med Mag. sc. A. Mentz har jeg udgivet „Planteverden i Menneskets Tjeneste" (Frem 1906) og det store Plancheværk „Billeder af Nordens Flora" (1901—1907). Endvidere har jeg publiceret en Række Afhandlinger og Artikler i inden- og udenlandske Fagtidsskrifter, omhandlende dels Plankton, dels floristiske og plantegeografiske Æmner vedrørende Karplanterne. Hertil kan føjes endnu i Gang værende Studier over Høgeurt (Hieracium)-Slægtens indviklede og afvigende Formeringsforhold (delvis i Samarbejde med Mag. sc. C. Raunkiær og Dr. O. Rosenberg fra Stockholm).

Afhandlingen „Plantevæxten paa Færøerne" forsvarede jeg 20. December 1906 for den filosofiske Doktorgrad. Den herved givne Lejlighed benyttede jeg til at paapege det ønskelige i, at Disputatser her i Danmark maatte kunne skrives og publiceres paa et Verdenssprog, saaledes som Tilfældet er i vore Nabolande Norge og Sverige; den ofte forekommende senere Udgivelse paa fremmed Grund og de ikke ringe Udgifter, der foraarsages ved at publicere samme Arbejde to Gange, vilde da spares.

I December 1900 indgik jeg Ægteskab med Inga Nyquist, Datter af Amtsdyrlæge Georg Nyquist i Norge og Hustru Barbara Obel.

IV.

Christian Ditlef Nielsen, Søn af Bryggersvend Johan Nielsen og Sofie N. f. Iversen, er født i København 4. Februar 1874. Min Skolegang afsluttede jeg i „De forenede Kirkeskoler" og tog i Aaret 1892 Artium som Privatist efter først at have forsøgt mig som Handelslærling i et Markfrø-Firma. I mine første Studenteraar dyrkede jeg moderne Sprog og havde forskellige Lærerpladser, et Aar var jeg saaledes Huslærer i et Køb-

mandshus paa Bornholm. Senere fik jeg Interesse for Theologie og østerlandske Sprog og tilbragte nogle fornøjelige Ungdomsaar paa Regensen som Theolog. Kammeratlivet med de danske Studenter paa Regensen og senere med de tyske i A. T. V. (Akadem. Turn Verein) hører til mine bedste Ungdomserindringer. Kampen om de bibelske Skrifters Ægthed vakte tidlig min Interesse og affødte i Foraaret 1899 mit første Indlæg i denne Strid: „Danielbogens Ælde belyst ved sproghistoriske Undersøgelser". Tre Maaneder efter tog jeg theologisk Embedsexamen (Laud) og fik i Aaret 1900 Rejsestipendier til fortsat Uddannelse i Udlandet, saa at jeg i $3^1/_2$ Aar kunde uddanne mig i semitisk Sprogvidenskab ved Universiteterne i Berlin, Marburg og München. Fra dette Tidsrum stammer: „Die altarabische Mondreligion und die mosaische Überlieferung", Strassburg, 1904, hvori jeg navnlig søgte at paavise Oprindelsen til vor ugentlige Hviledag. Min Værnepligt aftjente jeg som Fæstningsartillerist paa Middelgrundsfortet (1903—04) og fandt derefter et venligt Asyl paa Borchs Kollegium. Den 15. Juli 1905 giftede jeg mig med Elisabeth Henrichsen, Datter af Købmand F. Henrichsen i Maribo og Hustru Margrethe H. f. Werth. 19. December 1906 forsvarede jeg en sproglig Afhandling: „Studier over Oldarabiske Indskrifter" for den filosofiske Doktorgrad.

V.

Jeg, Gudmund Schütte, er født 17. Januar 1872. Min Fader, cand. jur. Ludvig Theodor Schütte, nu Ejer af Bygholm ved Horsens, er Søn af August Schütte (fra Perleberg i Mark Priegnitz) og Hansine Ammitzbøll, hvis Navn stammer fra Landsbyen Ammidsbøl ved Vejle. Min Moder Augusta Marie († 1896) var Datter af Overlæge ved Kastellet Jacob Petersen og Dorthea Knoph fra Kjøbenhavn. Min Fader, Farbroder cand. polit. Oscar S. og Broder cand. jur. Einar S. har alle matematisk Interesse i forskellige Retninger; min Fader har tillige sproglig-historisk Interesse. Jeg selv blev født paa min Faders Gaard Eskjær i Grinderslev Sogn (samt Tise Sogn)

paa Halvøen Salling, der hører til det vestjyske Dialektomraade. 1883—1889 gik jeg i Horsens Latinskole, hvor særlig Historielæreren, nuværende Overlærer Ludv. Schmidt, forstod at interessere mig. Min Interesse særskilt for Ætlæren (Etnologien) vaktes af Fr. Schiern's Bog „Europas Folkestammer", som jeg fandt paa Eskjær. I mine sidste Skoleaar lavede jeg et Atlas over Nationaliteternes Historie i Europa, tildels efter Stednavne. Ved Universitetet studerede jeg først Historie, men valgte siden Tysk, navnlig fordi Læreren i dette Fag, Professor Herman Møller, lagde stærk Vægt paa den ætniske Side, saaledes i sine Forelæsninger over Tacitus' Germania og over Gotiskens sproglige Stilling, hvoraf jeg har haft megen Nytte. I Aarene fra 1894 til 1896 tilbragte jeg tre Semestre ved Universitetet i Leipzig, hvor især Professor Edu. Sievers Forelæsning over Nibelung-Sagnet gjorde Indtryk paa mig; jeg studerede her sammen med Åge Meyer Benedictsen og nuværende Adjunkt Ernst Kaper. 1898 erhvervede jeg i Kjøbenhavn Universitetets Guldmedalje for en Afhandling om det angelsaxiske Sprogs Stilling og samme Aar tog jeg Magisterkonferens i Tysk. Paa min Doktorafhandling „Oldsagn om Godtjod" arbejdede jeg siden 1903; for Tilskyndelse og Raad skylder jeg særlig Tak til Docent Axel Olrik og Dr. phil. Henrik Bertelsen. For min Afhandling erhvervede jeg Doktorgraden d. 21. Marts 1907. Af andre omfangsrigere Afhandlinger har jeg skrevet forskellige: „Über die alte Geographie der nicht-klassischen Völker Europa's" (Indogermanische Forschungen 1903—1904; ɔ: metodiske Synspunkter for Forholdet mellem Samfærdselskresen og Synskresen); „Imperialisme og Kosmopolitisme" (Tilskueren 1903); „Om Racenavnet og Racetanken" (Tidskr. Norden 1904—1905); „Angantykvadets Geografi" (Ark. f. nord. filologi 1904); „En historisk Parallel til Nibelung-Sagnet" (smst. 1907). Til at knytte Forbindelse med forskellige Tidskrifter eller Udgiverværker har især Prof. Herman Møller hjulpet mig. I 1897 deltog jeg i Stiftelsen af „Selskab for germansk Filologi", for hvilket jeg fra 1898 til 1904 udgav en „Budstikke". I 1905—1906 var jeg sammen med Candd. polit. C. Thalbitzer og L. C. Schou Udgiver af „Akademisk Foreningsblad". — Mine

første Studieaar var ganske prægede af den ensidig germaniserende Aand, der har hersket blandt saa mange af vore yngre Videnskabsdyrkere. Dr. phil. H. J. Hansens Arbejde i engelsk Retning kendte jeg intet til; selv hans Skrift „Om Germanisering af dansk Videnskab" gik mig sporløst forbi. Senere er jeg ved Studium og Rejse kommen i Forbindelse med England, hvor jeg i H. M. Chadwick, Forfatter til „The Origin of the English Nation", har fundet en værdifuld Medforsker. I Norge har jeg fundet en lignende Medforsker i Dr. phil. Andreas M. Hansen, Forfatter til „Norsk Landnåm". Dengang „Selskab for germansk Filologi" stiftedes, var jeg med til officielt at godtage „Germaner" som vort ene rigtige Folkegruppenavn, og at vrage „Goter" som et „Paahit af Rasmus Rask". Senere opdagede jeg efterhaanden, at hine Meninger skyldtes ren Uvidenhed om de virkelige Forhold, idet nemlig Folkegruppenavnet Goter (eller Godtjod, Gottjod) fra Rask kunde følges helt tilbage til Eddaerne og de gamle Angelsaxer. Jeg opdagede, at især Rasks Lærling N. M. Petersen her som i hele Spørgsmaalet om de ætniske Forestillinger i deres Forhold til Samfærdselskresen og Synskresen havde seet adskillig klarere end min egen Samtid. At uddybe og metodisk klarlægge disse Iagttagelser blev Formaalet med mine Afhandlinger „Om Racenavnet og Racetanken" og „Oldsagn om Godtjod, vore Forfædres Land, Folk og Race".

VI.

Jeg, Hans Nicolaus Brix, er født i Vejle $^{24}/_{10}$ 1870. Forældre: Kaptajn, Skolebestyrer N. Brix og Hustru Anna Marie Ohrt.

Indtil 1884 gik jeg i Vejle Latinskole; jeg nød der Undervisning af saa fortræffelige Lærere som afdøde Skolebestyrer Slomann, Rektor Lund og min Fader, der var Skolens Matematiklærer. I 1884 flyttede mine Forældre til Varde, og jeg blev da sat i Ribe Latinskole, hvor jeg tilbragte tre Trængselsaar.

I 1887 blev jeg Student, og i 1894 tog jeg Skoleembeds-

examen med Dansk som Hovedfag; stor Tak skylder jeg Professorerne Paludan og Wimmer for disse Studieaar.

Siden har jeg været Lærer, fra 1906 ved Aalborg Katedralskole.

I 1903 ægtede jeg Johanne Scholl, født $^{6}/_{7}$ 1882, Datter af Apoteker H. D. Scholl i Struer.

I 1898 offentliggjorde jeg i Tidsskriftet Dania en Afhandling om Rimet i dansk Poesi. Jeg havde ikke tænkt oftere at skulle optræde som Forfatter, da jeg i 1905 svarede ja paa en tilfældig Opfordring til at skrive en Artikel om H. C. Andersens Poesi; jeg var nemlig da, i Hundredaaret fra Digterens Fødsel, bosat i Odense, hans Fødeby. Efter at den lille Afhandling var udkommet, fortsatte jeg mine Undersøgelser af Forholdet mellem Andersens Liv og Digtning, for om muligt at skaffe Løsningen paa den Række Gaader, det syntes at frembyde. En overordentlig Hjælp var det for mig, at Etatsraadinde Collin aabnede mig Adgang til de Collinske Samlinger.

I Sommerferien 1906 samlede jeg mine Resultater i en Afhandling: H. C. Andersen og hans Eventyr (Schubotheske Forlag), som jeg 22. Marts 1907 forsvarede for den filosofiske Doktorgrad.

For Tiden er jeg beskæftiget med at lave smaa Analyser af dansk Lyrik.

For Vennetjenester gennem Aarene takker jeg tre danske Doktorer: Marius Kristensen, Poul Levin og Vilhelm Andersen.

VII.

Jeg Johannes Peder Lindbæk er født i Ribe 6. December 1872, Søn af Adjunkt, senere Sognepræst i Seem, Jacob Borrig L., og Augusta Caroline f. Nielsen. Efter mine Forældres tidlige Død (1877 og 1878) blev jeg opdraget hos min Morfader, Branddirektør A. C. Nielsen i Varde. 1881—86 gik jeg i Varde Realskole, 1886—90 i Ribe Latinskole, hvorfra jeg tog Studenterexamen med 1. Kar. m. Udm. (107 Points). 1891 tog jeg Filosofikum med Udmærkelse.

Allerede som lille Dreng havde jeg haft en levende Interesse for Historie, og jeg valgte derfor at studere dette Fag (sammen med Fransk og Latin); jeg fik aldrig Grund til at fortryde dette Valg, da Universitetslærerne havde Ævne til baade at give os Unge Interesse for Faget og træde i nært personligt Forhold til os. Efter en fornøjelig Studentertid, hvoraf jeg tilbragte fire Aar (1893—97) paa Valkendorfs Kollegium, tog jeg Examen Jan. 1897 med 1. Kar. (112 Points). 1897—98 var jeg Lærer ved Birkerød Latin- og Realskole og opholdt mig de følgende tre Aar i Rom, hvor jeg med Understøttelse af Carlsbergfondet studerede i Vatikanets Arkiv. Denne Tid blev paa mange Maader af stor Betydning for mig, jeg blev ført til Interesse for Middelalderens Historie, især Kirkehistorie, og særlig gav en Forespørgsel fra daværende Borgmester, nu Stiftamtmand, Kammerherre Stemann, Anledning til, at jeg undersøgte det romerske Helligaandsklosters Arkiv, og at vi senere i Forening har udgivet en Bog om „De danske Helligaandsklostre" (1906). I andre Henseende førte Opholdet udenlands derimod til, at jeg forsømte nogle hjemlige Chancer. De første Aar efter min Hjemkomst var derfor paa flere Maader ret trange, da jeg maatte paatage mig for meget forskelligartet Arbejde, Undervisning og Foredrag ved Siden af mine videnskabelige Studier. Kun rigelig Understøttelse fra Universitetets Side (særlig det Regenburgske Legat) og en ny Rejse til Italien (Foraaret 1906) satte mig i Stand til at afslutte mit Arbejde „Pavernes forhold til Danmark under kongerne Kristiern I. og Hans",som jeg 26. Marts 1907 forsvarede for den filosofiske Doktorgrad.

1. Juli 1902 ægtede jeg Sofie Aubert, Datter af Professor L. M. B. Aubert i Kristiania og Forfatterinden Elise A., født Aars.

Foruden de to ovennævnte Arbejder har jeg udgivet:

Danske (og norske) besøgende i Hospitalet S. Maria dell' Anima i Rom (Kirk. Saml. 4. R. VI.).

Svenske i Rom (Svensk hist. Tidskr. 1902).

Oversigt over historisk litteratur vedrørende Sønderjylland. I. 1896—1900. II. 1901—03 (Sønderjydske Aarbøger 1903 og 1906).

Dorothea, Kristiern den førstes dronning, og familien Gonzaga (Hist. Tidsskr. 7. R. III.).

Biskop Niels Skave i Roskilde og Sorø kloster (Hist. Tidsskr. 8. R. I.).

Aktstykker og Oplysninger til Statskollegiets Historie. 1ste Bind. 1660—70. (1903—05).

I Samarbejde med Underbibliotekar Alfr. Krarup: Acta pontificum Danica II. 1378—1431. (1907).

Desuden Artikler i Salmonsens Konversationslexikon, Anmeldelser i Historisk Tidsskrift og „Dannebrog" m. m.

VIII.

Jeg, Christian Leschly Heyerdahl, er født paa Fredriksberg $^{9}/_{12}$ 1869, Søn af Grosserer Christian Julius Halfdan Heyerdahl og Marie Heyerdahl f. Leschly, dimitteret fra Metropolitanskolen 1887, Candidat fra Sommeren 1893.

Fra Maj—December 1895 var jeg Læge ved Thingvallalinien, studerede Massage i Stockholm i Foraaret 1896; efter Hjemkomsten herfra var jeg Kandidat paa Frederiksberg Hospital indtil Januar 1898, og derefter paa Kommunehospitalet indtil September 1899.

Efter at have fuldendt min Hospitalsuddannelse har jeg dels beskæftiget mig med almindelig Praxis, dels sammen med min Kollega Frode Sadolin udøvet en ret betydelig Massagevirksomhed, under hvilket Arbejde de Erfaringer er høstede, som ligger til Grund for min Afhandling om den nervøse Hovedpine.

IX.

Otto Valdemar Christian Emil Petersen er født d. 10de October 1875, Søn af Skoleinspektør cand. theol. J. P. V. Petersen og Hustru Martha Amalie f. Lange.

Student fra Borgerdydsskolen i Helgolandsgade Sommeren 1893 (laudabilis), examen philosophicum Sommeren 1894 (godt), medicinsk Forberedelsesexamen Sommeren 1895. Allerede som Student interesserede jeg mig særligt for Anatomi og udførte, dels før jeg havde taget 1ste Del af Embedsexamen, dels mel-

lem denne og anden Del, adskillige Præparater til normal-anatomisk Musæum.

Sommeren 1900 absolverede jeg medicinsk Embedsexamen med Karakteren laudabilis. Jeg var i April samme Aar bleven ansat som Assistent ved normal-anatomisk Musæum, og denne Plads beholdt jeg, indtil jeg 1ste Februar 1902 ansattes som Prosector anatomiæ. Fra 1ste Juli 1900 til 1ste Februar 1902 var jeg Candidat paa Sct. Johannesstiftelsens Sygehus i København.

Som Skibslæge i Skandinav. Amerikalinjen har jeg paa S/S Hekla besøgt New York i Juni 1904, paa S/S Oscar II Hamburg i Januar 1906 og endelig atter været i New York Juli 1906 paa S/S C. F. Tietgen. Juni 1906 Studieophold i Berlin og Rostock for Thomas Finch's Rejsestipendium.

Efter at jeg fra 1ste Februar 1907 var ophørt med at være Prosector anatomiæ, er jeg fra 1ste April ansat som fast Lægecandidat paa Kommunehospitalet i København. Tillige fungerer jeg fra 1ste Februar 1907 som Assistent paa normal-anatom. Musæums Studiesal.

28. Juni 1907 forsvarede jeg en Afhandling, betitlet: „Bidrag til den mikroskopiske Anatomi af vesicula seminalis hos Mennesket og nogle Pattedyr", for den medicinske Doktorgrad.

Jeg har tidligere offentliggjort:

Ueber die Lagerung des Glycogens in den Leberzellen beim Kaninchen. Anatom. Anzeiger 1904.

Ueber Articulationsflächen an der Hinterfläche des os sacrum. Anatom. Anzeiger 1905.

Ueber secretorische Aenderungen im Epithel der ableitenden Harnwege bei einigen Säugetieren. Anatom. Anzeiger 1905.

Den 30te Juni 1906 indgik jeg Ægteskab med Jacoba Ernestine Elisabeth Øst, Datter af Inspektør Alexander Christian Øst og Hustru Bertha Caroline Augusta, født Bøckmann.

X.

Carl Theodor Jacobsen er født d. 18. Februar 1869 i Ordrup, Krogstrup Sogn, Søn af Gaardejer Niels Jacobsen og Hustru Laura Smith.

Jeg gik i Almueskole til 12 Aars Alderen, derefter i Roskilde Katedralskole, hvorfra jeg blev Student med 1. Karakter i 1888. Af min Studentertid var jeg de sidste $2^1/_2$ Aar Alumnus paa Regensen. I Sommeren 1895 fik jeg medicinsk Embedsexamen med laud. Derefter frekventerede jeg forskellige Klinikker i København og havde et Par kortvarige Vikariater paa Landet, indtil jeg i December 1895 nedsatte mig som praktiserende Læge ved Havdrup Station. I 1898 tog jeg igen til København og var i Foraaret 1899 Deltager i et Kursus i Hygiejne paa Universitetets hygiejniske Laboratorium, hvor jeg nogen Tid efter begyndte paa de Undersøgelser, som jeg har nedskrevet i min Doktordisputats, „Undersøgelser over Tyfusbacillen".

Fra Marts 1899 til Februar 1900 var jeg Reservelæge paa Garnisonssygehus i København og umiddelbart derefter fast Kandidat paa Kommunens Hospitaler til December 1901, da jeg nedsatte mig som praktiserende Læge paa Vesterbro. Fra Januar 1902 til Maj 1904 var jeg Assistent paa Poliklinikkens Afdeling for Øre-, Næse- og Halssygdomme.

I Maj 1904 fik jeg Udnævnelse som Korpslæge i Hæren og flyttede til Aarhus, hvor jeg siden har praktiseret.

D. 9. Maj 1904 ægtede jeg Frøken Elna Ketty Ingeborg Berg, Datter af fhv. Købmand Frederik Berg.

Studierejse til Tyskland i Juli og August 1907.

XI.

Hans Christian Winther, Søn af Bankdirektør, fhv. Købmand Mads Christian Anthon Winther og Hustru Marie, f. Madsen, er født i Rudkøbing d. 4de Juli 1873. Tog Præliminærexamen fra Rudkøbing Realskole 1888, matematisk Artium fra Aarhus Kathedralskole 1891 og Magisterkonferens i Kemi 1897. Maj 1899 blev jeg Assistent ved Universitetets kemiske Laboratorium, hvor jeg endnu har Ansættelse. I Maj 1900 ægtede jeg Ellen Christine Vognsen, Datter af afd. Bankdirektør V. i Rudkøbing, i hvilket Ægteskab jeg har en Datter.

I 1903 arbejdede jeg et Semester paa W. Ostwalds fysikokemiske Laboratorium i Leipzig, og i 1906 foretog jeg med

Understøttelse fra Kommunitetet en Rejse i videnskabeligt Øjemed gennem England, Holland, Tyskland og Schweiz.

Allerede i min Studietid blev min Interesse vakt for de optisk aktive Stoffers Ejendommeligheder, hvoraf resulterede to teoretiske Arbejder: „Zur Theorie der Spaltungen der razemischen Formen" (1895) og „Æblesyrens optiske Forhold" (1896). Efter at jeg ved Carlsbergfondets Hjælp — hvorfor jeg vel navnlig kan takke den overordentlige Velvilje, hvormed min højtagtede Lærer, Prof., Dr. S. M. Jørgensen, stedse har fulgt mine Arbejder — var bleven forsynet med gode Instrumenter, kunde jeg trænge dybere ind paa det nævnte Felt, hvoraf resulterede en Række, tildels experimentelle Arbejder, udgivne dels paa Dansk i Videnskabernes Selskabs Skrifter, dels paa Tysk, nemlig: „Ueber eine leicht herstellbare Cuvette für Strahlenfilter" (1902); „Rotationsdispersionen hos de spontant aktive Stoffer" (1902); „Rotationsdispersionen i Opløsninger" (1903); „Einige Bemerkungen üb. das Drehungsvermögen optisch aktiver Körper" (1905); „Studien über katalytische Razemisirung" (1906), hvilket sidste Arbejde skaffede mig Videnskabernes Selskabs Guldmedalje. Resultaterne af mine og andres Arbejder har jeg sammenfattet i 3 teoretiske Arbejder, nemlig: „Zur Theorie d. optischen Drehung" I og II (1906) og „Bidrag til den optiske Drejnings Teori" (1907), hvilket sidste Arbejde jeg forsvarede for Doktorgraden d. 13de September 1907.

Sammen med O. B. Bøggild har jeg endvidere skrevet: „On some minerals from the nephelite-syenite at Julianehaab" (1900).

Foruden enkelte populære Skrifter og Tidsskriftsartikler har jeg i Undervisningsøjemed skrevet en „Lærebog i analytisk Kemi" 1ste Udg. 1905, 2den Udg. 1907, som benyttes paa Universitetets kemiske Laboratorium og flere andre Steder, samt „Det theoretiske Grundlag for den analytiske Kemi" (1902).

XII.

Borgbjærg, Axel Hedegaard Jeppesen (Borgbjærg ifølge navnebevilling af 3die maj 1890), er født den 27de juni 1868 i Boeslunde ved Korsør.

Søn af afdøde dyrlæge J. Jeppesen og hustru Hermine Dorothea f. Hedegaard.

Student 1887 fra Nykøbing kathedralskole (1ste karakter).

Medicinsk embedseksamen (laudabilis) vinteren 1894.

Kandidat på Kommunehospitalet februar 1894 til februar 1895.

Praktiserende læge i Eskildstrup på Falster fra marts 1895 til februar 1900.

Studerede derpå fordøjelsessygdomme, særlig i Tyskland.

Siden februar 1901 praktiseret som specialist i fordøjelsessygdomme i København.

Dr. med. 10de oktober 1907 (Ventrikelfunktionsundersøgelsens betydning for diagnosen af ulcus ventriculi").

Gift 19. juni 1896 med Johanne Juliane Mathiesen, datter af sognepræst C. E. Mathiesen, Reerslev pr. Hedehusene, og hustru Louise f. Blicher.

XIII.

Valdemar Johannes Hansen Harsløf er født d. 5. Oktober 1867 paa Ødegaard ved Saxkjøbing under Baroniet Guldborgland og Lehn som yngste Søn af afdøde Forpagter Julius Wilhelm Hansen og Hustru Ida Sofie Birgitte født Friis. 1886 dimitteredes jeg fra Latinskolen i Nykjøbing Falster som Student med 1. Karakter. Ved Universitetet studerede jeg først Theologi og absolverede i Sommeren 1892 theologisk Embedsexamen med Haud I. Efter at have aftjent Værnepligten paabegyndte jeg i Marts 1893 — da jeg, som overbevist Christen, af ideelle Grunde ikke følte Kald til Præstegerning — det medicinske Studium, som jeg tilendebragte i Januar 1898 med Laud. I de følgende Aar til 1904 incl. completterede jeg min Uddannelse som Læge rundt paa de københavnske Hospitaler, samt i Randers som Reservelæge i 2 Aar, 1900 og 1901 og i Dresden i 99. Siden 1904 praktiserer jeg i Brønshøj. 17. Oktober 1907 forsvarede jeg min Afhandling: „Den operative Behandling af Ulcus ventriculi, dets Complicationer og nærmeste Consequenser, et Afsnit af Ventrikelchirurgiens

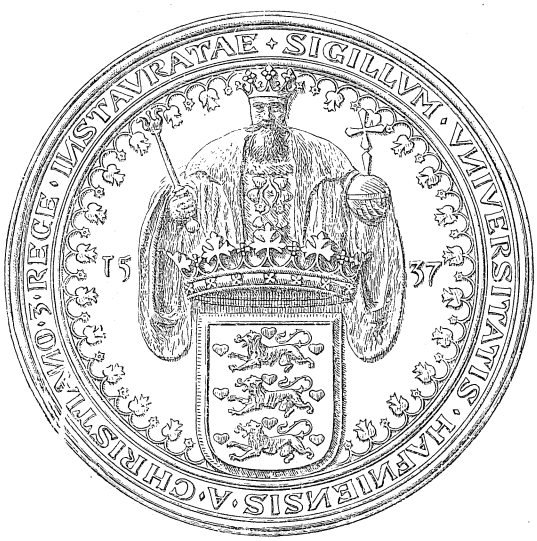
nuværende Stilling i Danmark" — for den medicinske Doctorgrad.

8. Maj 1900 erholdt jeg kgl. Bevilling til fremtidig at føre Slægtsnavnet „Harsløf". 11. Maj 1900 ægtede jeg i Majbølle Kirke (Lolland) Julie Dagmar Vett f. 29. Marts 1872 i Guldborg, Lolland, Datter af Købmand Herman Rudolph Vett og Hustru Caroline Mathilde f. Fæster, i hvilket Ægteskab er født 2 Sønner og 1 Datter nemlig Bjørn Valdemarssøn Harsløf, f. 5. Juli 1901, Valdemar Valdemarssøn Harsløf, f. 17. Februar 1904 og Estrid Valdemarsdatter Harsløf, f. 4. Juni 1906.

Universitetets Aarsfest vil blive afholdt i Universitetets Festssl Torsdagen den 21de November Kl. 12. Talen holdes af Prof. Dr. phil. & math. H. G. Zeuthen. Efter denne Tale vil Universitetets Rektor, Prof. Dr. phil. M. Cl. Gertz give en kort Oversigt over, hvad der har tildraget sig ved Universitetet i det nu fuldendte Aar, samt proklamere prakt. Læge i Kjøbenhavn Chr. L. Heyerdahl, Cand. med. O. V. Chr. E. Petersen, Korpslæge C. Th. Jacobsen, prakt. Læge i Kjøbenhavn A. H. J. Borgbjærg og prakt. Læge i Brønshøj V. J. H. Harsløf som Doktorer i Medicinen, Cand. mag. K. Fr. K. Fabricius, Assistent ved Universitetets zoologiske Museum, Mag. sc. A. G. Bøving, Inspektør ved Universitetets botaniske Haves Museum, Mag. sc. C. E. H. Ostenfeld, Cand. theol. C. D. Nielsen, Mag. art. G. Schütte, Adjunkt ved Aalborg Kathedralskole Mag. art. H. N. Brix, Cand. mag. J. P. Lindbæk og Assistent ved Universitetets kemiske Laboratorium, Mag. sc. H. Chr. Winther som Doktorer i Filosofien, hvorefter han overgiver Rektoratet til den for næste Aar valgte Rektor, Prof. Dr. phil. J. E. B. Warming. Samtidig overtages Dekanatet i det theologiske Fakultet af Prof. Dr. theol. P. Madsen, i det rets- og statsvidenskabelige af Prof. jur. J. S. V. Lassen, i det lægevidenskabelige af Prof. Dr. med. H. C. J. Gram, i det filosofiske

af Prof. Dr. phil. & litt. J. L. Heiberg og i det mathematisk-naturvidenskabelige af Prof. Dr. phil. N. V. Ussing.

Ved Festen afsynges den til Universitetets Reformationsfest forfattede Kantate af J. L. Heiberg med Musik, komponeret af C. E. F. Weyse.

Kjøbenhavn, den 15de November 1907.

Under Universitetets Segl.